

FULLY HILBERTIAN FIELDS

LIOR BARY-SOROKER AND ELAD PARAN

ABSTRACT. We introduce the notion of fully Hilbertian fields, a strictly stronger notion than that of Hilbertian fields. We show that this class of fields exhibits the same good behavior as Hilbertian fields, but for fields of uncountable cardinality, is more natural than the notion of Hilbertian fields. In particular, we show it can be used to achieve stronger Galois theoretic results. Our proofs also provide a step toward the so-called Jarden-Lubotzky twinning principle.

1. INTRODUCTION

A field K is called Hilbertian if it satisfies the following property: for every irreducible polynomial $f(X, Y) \in K[X, Y]$ which is separable in Y , there exist infinitely many $a \in K$ for which $f(a, Y)$ is irreducible in $K[Y]$. The name Hilbertian is derived from Hilbert's irreducibility theorem, which asserts that number fields are Hilbertian.

Hilbert's original motivation for his irreducibility theorem was the inverse Galois problem. Assume one wants to realize a finite group G over a Hilbertian field K . Then given a regular Galois extension $F/K(x)$ with group G , one can use Hilbert's irreducibility theorem to specialize x to $a \in K$ and obtain a Galois extension \bar{F} of K with group G . Moreover, there exist infinitely many such specialized fields, linearly disjoint over K , obtained by suitable choices of $a \in K$. Even nowadays Hilbert's irreducibility theorem remains a central approach for the inverse Galois problem, see [16, 22]. Moreover, this theorem has numerous other applications in number theory, see e.g. [21].

It is yet unknown if the inverse Galois problem has a positive solution over a Hilbertian field K , or equivalently, if it has a positive solution over $K(x)$. If a field K is ample (e.g. K is algebraically closed, PAC, or Henselian) then a theorem of Pop asserts that the inverse Galois problem has a positive solution over $K(x)$. Thus the inverse Galois problem has a positive solution over ample Hilbertian fields.

The cardinality of the set of solution fields \bar{F} to each instance of the inverse Galois problem affects the structure of the absolute Galois group of the field K . Surprisingly, if K is uncountable, it might happen that a regular Galois extension $F/K(x)$ has only countably many specialized solutions \bar{F} (see Example 2.2). Moreover, in order to study the absolute Galois group, one needs to study not only the possible realizations of finite groups, but also how the obtained fields fit together. This is achieved using finite embedding problems, which give rise to non-regular extensions of $K(x)$.

More precisely, let $f(X, Y)$ be an irreducible polynomial that is separable in Y . Let $F = K(X)[Y]/(f(X, Y))$ and let L be the algebraic closure of K in F . Each a in the corresponding Hilbert set $H(f) = \{a \in K \mid f(a, Y) \text{ irreducible}\}$ provides a specialized field \bar{F}_a that contains L with degree $[\bar{F}_a : K] = [F : K]$. If $F = L(X)$, then $L = \bar{F}_a$ for all a , i.e., L is the unique specialized field. In the non-trivial case, Hilbertianity implies the existence of infinitely many specialized fields that are linearly disjoint over L . However, as mentioned above, even if K is uncountable it is possible that there exist only countably many such fields (and even though the cardinality of $H(f)$ always equals that of K).

In this work we study fields which have as much and as distinct as possible specialized fields \bar{F}_a . That is to say, there exists a subset $A \subseteq H(f)$ of cardinality $|K|$ such that the specialized fields \bar{F}_a are linearly disjoint over L (where a runs over A). We call a field with this feature **fully Hilbertian**. It is important to note that a *countable* field K is Hilbertian if and only if it is fully Hilbertian. In particular, number fields are fully Hilbertian.

The objective of this work is to initiate the study of fully Hilbertian fields. Therefore we give several equivalent definitions of fully Hilbertian fields, construct many fundamental examples of fully Hilbertian fields, and study the behavior of this notion under extensions. We also show how one can apply this notion and obtain strong Galois theoretic results over fields of large cardinality. We note that as Hilbert's irreducibility theorem found many other applications outside the scope of Galois theory, this notion may be useful for other problems over uncountable fields.

1.1. Characterizations of fully Hilbertian fields. A recent characterization of Hilbertian fields by the first author [3] reduces the Hilbertianity property to absolutely irreducible polynomials. We show that a similar property holds for fully Hilbertian fields:

Theorem 1.1. *The following are equivalent for a field K .*

- (a) *K is fully Hilbertian.*
- (b) *For every absolutely irreducible $f(X, Y) \in K[X, Y]$ that is separable in Y there exist $|K|$ many $a \in H(f)$ and b_a a root of $f(a, Y)$ such that $K(b_a)$ are linearly disjoint over K .*
- (c) *For every finite Galois extension $F/K(x)$ with L the algebraic closure of K in F , there exist $|K|$ many $a \in K$ such that $[\bar{F}_a : K] = [F : K]$ and all \bar{F}_a are linearly disjoint over L .*

1.2. Finitely generated field extensions. The most fundamental family of Hilbertian fields is the family of number fields. As mentioned above, since countable Hilbertian fields are fully Hilbertian, number fields are fully Hilbertian. The second important family is that of function fields:

Theorem 1.2. *Let F be a finitely generated transcendental extension of an arbitrary field K . Then F is fully Hilbertian.*

1.3. Extensions of fully Hilbertian fields. Hilbertian fields have interesting behavior under algebraic extensions which has been well studied; [6, Chapter 13] offers a good treatment of this subject. We show that fully Hilbertian fields exhibit the same behavior.

Any algebraic extension L/K factors into a tower of fields $K \subseteq E \subseteq L$ in which E/K is purely inseparable and L/E is separable. We study each case separately. First, full Hilbertianity is preserved under purely inseparable extensions:

Theorem 1.3. *Let E be a purely inseparable extension of a fully Hilbertian field K . Then E is fully Hilbertian.*

The case of separable extensions is much more interesting. First, it is clear that not every extension of a fully Hilbertian (or Hilbertian) field is Hilbertian. For example, a separably closed field is not Hilbertian, and hence not fully Hilbertian. The most general result for Hilbertian fields is Haran's diamond theorem [10]. We prove an analog of the diamond theorem, and all other permanence criteria for fully Hilbertian fields.

Theorem 1.4. *Let M be a separable extension of a fully Hilbertian field K . Then each of the following conditions suffices for M to be fully Hilbertian.*

- (a) M/K is finite.
- (b) M is an abelian extension of K .
- (c) M is a proper finite extension of a Galois extension N of K .
- (d) (The diamond theorem) there exist Galois extensions M_1, M_2 of K such that $M \subseteq M_1 M_2$, but $M \not\subseteq M_i$ for $i = 1, 2$.

(Our full result appears in Section 4.2.)

In order to prove Theorem 1.4 we identify and exploit a connection between fully Hilbertian fields and so-called semi-free profinite groups. This is a refinement of the **twinning principle** [15] suggested by Jarden and Lubotzky. They note a connection between results about freeness of subgroups of free profinite groups and results about Hilbertianity of separable extensions of Hilbertian fields. Furthermore, Jarden and Lubotzky state that the proofs in both cases have analogies. In spite of that they add that *it is difficult to see a real analogy between the proofs of the group theoretic theorems and those of field theory*.

In [9, 10] Haran provides more evidence to the twinning principle by proving his diamond theorem in both cases (see also [6, Theorems 13.8.3 and 25.4.3]). Haran's main tool in both proofs is twisted wreath products. (Using twisted wreath product one can induce embedding problems and then, on the other direction, induce weak solutions via Shapiro's map. Haran shows that under some conditions those weak solutions are in fact solutions, i.e., surjective. We refer to this method henceforth as the **Haran-Shapiro induction**.)

In this work we prove all the permanence results for fully Hilbertian fields by reducing them to the group theoretic case. In fact we show that any group theoretic result obtained via the Haran-Shapiro induction transfers an analogous field theoretic result. First we explain why a better analogy is between *semi-free profinite* groups of rank m and *fully Hilbertian* fields of cardinality m^1 . A semi-free group is, in a sense, a free group without projectivity, i.e., a semi-free projective group is free. These groups recently appeared with connection to Galois theory, see [4].

¹If one wants to consider only Hilbertian fields, then our work shows the connection between Hilbertian fields and profinite groups having the property that any finite split embedding problem is solvable.

The idea of the proof is to show that all the constructions in the Haran-Shapiro induction are “field theoretic”. This is based on the theory of rational embedding problems and geometric solutions developed in the first author’s PhD dissertation, see [2].

Then all the permanence results about semi-free profinite groups of [4] carry over to fully Hilbertian fields, proving Theorem 1.4. To the best of our knowledge, this is the first time a reduction from the field theoretic case to its group theoretic counterpart has been made. We hope this is a step towards a rigorous formulation of the twinning principle.

1.4. Galois theory of complete local domains. Complete local domains play an important role in number theory and algebraic geometry, and their algebraic properties have been described by Cohen’s structure theorem in 1946. However, the Galois theoretic properties of their quotient fields have only recently been understood. The first result in this direction has been made in [12], where Harbater-Stevenson essentially prove that the absolute Galois group of $K = K_0((X, Y))$ is semi-free of rank $|K|$, for an arbitrary base field K_0 (see also [4]). The general case was treated independently by Pop [20] and the second author [18]:

Theorem 1.5. *Let K be the quotient field of a complete local domain of dimension exceeding 1. Then $\text{Gal}(K)$ is semi-free of rank $|K|$.*

The fields K in the above theorem are ample [20]. For such fields, we have the following result:

Theorem 1.6. *If K is a fully Hilbertian ample field, then $\text{Gal}(K)$ is semi-free of rank $|K|$.*

We prove a stronger results about these, namely their maximal purely inseparable extension is fully Hilbertian.

Theorem 1.7. *Let K be the quotient field of a complete local domain of dimension exceeding 1. Then the maximal purely inseparable extension K_{ins} of K is fully Hilbertian.*

Note that if K is of characteristic 0, then K itself is fully Hilbertian.

Theorem 1.7 provides a new proof of Theorem 1.5 since $\text{Gal}(K) = \text{Gal}(K_{\text{ins}})$. However, we note that Theorem 1.7 is stronger than Theorem 1.5, since there exist ample fields of any characteristic with semi-free absolute Galois group that are not fully Hilbertian (Remark 2.14).

We do not know in general whether K is fully Hilbertian or not. Our key result states that there is $A \subseteq K$ of independent irreducible specializations provided that all the ramification points are separable over K .

To prove Theorem 1.7 we use the Hilbertianity of K . Using the density theorem of Hilbertian sets, we find irreducible specializations with the following nice feature. The geometric inertia groups of the function fields are “specialized” to inertia groups of valuations of K .

During the Oberwolfach workshop on the arithmetic of fields after reporting this work, we learned from Pop, that he uses a similar approach to prove Theorem 1.5.

Acknowledgment. We wish to thank Arno Fehm, Dan Haran, Moshe Jarden, and Franz-Viktor Kuhlmann for useful discussions about this work.

2. EMBEDDING PROBLEMS, HILBERTIAN FIELDS, AND FULLY HILBERTIAN FIELDS

2.1. Fully Hilbertian fields in terms of polynomials. Recall that, for an irreducible polynomial $f(X, Y) \in K[X, Y]$ that is separable in Y , the Hilbert set $H(f) \subseteq K$ is the set of all $a \in K$ such that $f(a, Y)$ is irreducible. It will be convenient sometimes to restrict to the co-finite subset $H'(f) \subseteq H(f)$ of all $a \in H(f)$ for which $\deg f(a, Y) = \deg_Y f(X, Y)$ and $f(a, Y)$ separable. By definition K is Hilbertian if and only if all Hilbert sets are non-empty, and hence infinite. In fact the cardinality of each Hilbert set must be as large as possible.

Proposition 2.1 (Jarden). *Let K be a Hilbertian field and $H = H(f)$ a Hilbert set over K . Then $|H| = |K|$.*

Proof. If K is countable the result is trivial.

Assume $m = |K| > \aleph_0$. Let $\{t_i \mid i \leq m\}$ be a transcendence basis of K over its prime field K_0 . Define a valuation v on $K_0(t_i \mid i \leq m)$ inductively such that $v(t_1) = 1$ and

$$j < i \longrightarrow v(t_j) > v(t_i).$$

We have $v(t_i - t_j) = v(t_i) \leq v(t_1) = 1$, for all $j < i \leq m$. Extend v to K arbitrarily.

For each $i < m$ let $B_i = \{x \in K \mid v(x - t_i) > 1\}$ be an open ball. If $x \in B_i$, then $v(x) = v(x - t_i + t_i) = v(t_i)$. This implies that these balls are disjoint. The proof is now done, since H is dense in the topology defined by v [7, Lemma 4.1]. \square

Let us now focus on the fields generated by a root of $f(a, Y)$ where a varies over $H(f)$. The last result asserts that $|H(f)| = |K|$, hence it is somewhat surprising that the cardinality of the set of fields generated by a root of $f(a, X)$, $a \in H(f)$ can be smaller than $|K|$. The following example gives a Hilbertian field K such that $|K| > \aleph_0$, but the cardinality of the set of specialized fields is countable.

Example 2.2 (Jarden). Let K be a pseudo algebraically closed (PAC) field with free absolute Galois group of rank $> \aleph_0$. Then $|K| > \aleph_0$. Now the free profinite group G of countable rank is a subgroup of $\text{Gal}(K)$; let L be its fixed field. Then $\text{Gal}(L) = G$. By [6, Corollary 11.2.5] L is PAC. Clearly $|L| = |K|$. Furthermore, L is Hilbertian, as an ω -free PAC field [6, Corollary 27.3.3].

Every finite separable extension of L corresponds to an open subgroup of G . But the rank of G is countable; hence G has only countably many open subgroups, and thus there are only countably many fields generated by roots of $f(a, Y)$, $a \in H(f)$.

We will use the following notation: Let K be a field and fix a separable closure K_s of K . Consider an irreducible polynomial $f(X, Y) \in K[X, Y]$ that is separable in Y (i.e. $\frac{\partial f}{\partial Y} \neq 0$). Let $E = K(X)[Y]/(f(X, Y))$. Then $E/K(X)$ is a finite separable extension. Let $L = E \cap K_s$ be the algebraic closure of K in E .

For every $a \in H'(f)$ there is a unique prime \mathfrak{p} of E/L lying above $(X - a)$. However the residue field E_a of E under \mathfrak{p} is not unique. Since we already fixed E and K_s , and hence L ,

E_a is unique up to an element $\sigma \in \text{Gal}(L)$. In any rate, $L \subseteq E_a$ independent of the choice of E_a . We define fully Hilbertian fields to have as much as possible specialized fields that are linearly disjoint over L .

Definition 2.3. A field K is called fully Hilbertian if for every $f(X, Y)$ the following property holds. Let $E = K(X)[Y]/(f(X, Y))$ and $L = E \cap K_s$. Then there exists a set $A \subseteq H(f)$ of cardinality $|A| = |K|$ and a set of specialized fields $\{E_a \mid a \in A\}$ that are linearly disjoint over L .

Remark 2.4. If $E \cong L(X)$, then $E_a = L$, for all a . However, formally, L is linearly disjoint of L over L . So in this trivial case, there always exists a set A as in the definition.

Remark 2.5. Definition 2.3 is the most naïve definition. The definition is not canonical, in the sense that there are many choices of the fields E_a . This will be solved below, when we give a characterization of fully Hilbertian fields in terms of Galois extensions $E/K(X)$, or more accurately, in terms of rational embedding problems.

We give a weaker definition of a ‘regular fully Hilbertian’ field. Later we prove that in fact it is the same notion as fully Hilbertian, cf. [3] for the classical case.

Definition 2.6. A field K is called **regular fully Hilbertian** if for any absolutely irreducible polynomial $f(X, Y)$ there exists a set $A \subseteq H(f)$ of cardinality $|A| = |K|$ and for each $a \in A$, a root b_a of $f(a, X)$ such that the fields $K(b_a)$, $a \in A$ are linearly disjoint over K .

Remark 2.7. It is natural to consider Galois fully Hilbertian fields – fields having the strong specialization property for every irreducible polynomial $f(X, Y)$ separable and Galois in Y . before doing so, we introduce some useful terminology.

2.2. Embedding problems. The following notions of rational embedding problem and geometric solutions are essential in this work, cf. [2]. Recall that an **embedding problem** for a field K is a diagram

$$\begin{array}{ccc} & & \text{Gal}(K) \\ & & \downarrow \nu \\ B & \xrightarrow{\alpha} & A, \end{array}$$

where B, A are profinite groups and α, ν are (continuous) epimorphisms. The embedding problem is **finite** (resp. **split**) if B is finite (resp. α splits). It is **non-trivial** if α is not isomorphism, or equivalently, $\ker \alpha \neq 1$.

A **weak solution** of (ν, α) is a homomorphism $\theta: \text{Gal}(K) \rightarrow B$ such that $\theta\nu = \alpha$. If θ is also surjective, we say that θ is a **proper solution**, or in short **solution**.

We can always replace A with $\text{Gal}(L/K)$, where $\text{Gal}(L) = \ker \nu$ and ν with the restriction map to get an equivalent embedding problem.

In what follows we show that B can also be considered as a Galois group of some geometric object. In fact, the interesting object of study are the geometric embedding problems.

Definition 2.8. Let E be a finitely generated regular transcendental extension of K , let F/E be a Galois extension, and let $L = F \cap K_s$. Then the restriction map $\alpha: \text{Gal}(F/E) \rightarrow \text{Gal}(L/K)$ is surjective, since $E \cap K_s = K$. Therefore

$$(1) \quad (\nu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/E) \rightarrow \text{Gal}(L/K))$$

is an embedding problem for K . We call such an embedding problem a **geometric embedding problem**.

If $E = K(x_1, \dots, x_d)$ is a field of rational functions over K then we call (1) a **rational embedding problem**.

Remark 2.9. In the definition the transcendence degree d of E/K can be arbitrary. However, in the setting of this work, it suffices to consider only the case $d = 1$. This observation is based on the Bertini-Noether lemma and the Matsusaka-Zariski theorem, see [6, Proposition 13.2.1] or [3, Lemma 2.4].

Remark 2.10. In [6, Lemma 11.6.1] it is shown (in different terminology) that every finite embedding problem for a field K is equivalent to a geometric embedding problem.

We shall see below that if K is infinite, then any rational embedding problem has a weak solution. Hence the existence of a weak solution is necessary for an embedding problem to be equivalent to a rational embedding problem. A central result in Galois theory of Pop [19] asserts that if K is ample, then every finite split embedding problem over K is regularly solvable, and in our terminology, equivalent to a rational embedding problem.

In fact the regularity of finite split embedding problems immediately implies that the above necessary condition, i.e., existence of a weak solution, also suffices for an embedding problem over an ample field to be regularly solvable. See Lemma 2.12.

The next natural step is to consider solutions to geometric embedding problems that come from field theory, i.e., are defined by places. Before giving the definition, we introduce additional notation. Let E/K be an extension of fields and let φ be a place of E . We say that φ is a K -place if $\varphi|_K = \text{id}_K$. We denote by \bar{E}_φ (or simply \bar{E} if there is no risk of confusion) the residue field of E under φ .

Definition 2.11. Consider a geometric embedding problem (1). Let φ be a K -place of E and let Φ be an extension of φ to an L -place of F . Assume that

- (a) $\bar{E} = K$ and
- (b) Φ/φ is unramified.

Then the decomposition group $D = D_{\Phi/\varphi}$ is isomorphic to $\text{Gal}(\bar{F}/K)$ (for a proof, apply [6, Lemma 6.1.4] to the valuation rings of Φ/φ). Thus we have a canonical map $\Phi^*: \text{Gal}(K) \rightarrow \text{Gal}(F/E)$ whose image is D . Clearly $\Phi^*\nu = \alpha$, since Φ^* respects the restriction maps (recall that ν is a restriction map). In other words Φ^* is a weak solution of (1).

Let $\theta: \text{Gal}(K) \rightarrow \text{Gal}(F/E)$ be a weak solution of (1). We say that θ is **geometric**, if there exists Φ/φ satisfying (a) and (b) for which $\theta = \Phi^*$.

The following lemma shows that if we take ‘larger’ or ‘smaller’ embedding problems from a given rational embedding problem, the new ones are also rational.

Lemma 2.12. *Let $(\nu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K))$ be a rational embedding problem for a field K .*

- (a) *If $\alpha = \beta\gamma$, for some epimorphisms $\gamma: \text{Gal}(F/K(x)) \rightarrow B$, $\beta: B \rightarrow \text{Gal}(L/K)$, then (ν, β) is rational.*
- (b) *Let Φ^* be a geometric weak solution of (ν, α) . Then $\gamma\Phi^*$ is a geometric weak solution of (ν, β) .*
- (c) *Let N be a Galois extension of K that contains L , let $\mu: \text{Gal}(K) \rightarrow \text{Gal}(N/K)$ be the restriction map, let $C = \text{Gal}(F/K(x)) \times_{\text{Gal}(L/K)} \text{Gal}(N/K)$ be the fiber product, and let $\delta: C \rightarrow \text{Gal}(N/K)$ and $\epsilon: C \rightarrow \text{Gal}(F/K(x))$ be the quotient maps. Then there exists a natural isomorphism $C \cong \text{Gal}(FN/K(x))$ under which δ, ϵ are the restriction maps. In particular, (μ, δ) is rational.*
- (d) *Let Φ be an N -place of FN which is unramified over $K(x)$. If $\theta = \Phi^*$ is a weak geometric solution of (μ, β) , then $\epsilon\theta = (\Phi|_F)^*$. In particular, $\epsilon\theta$ is a weak geometric solution of (ν, α) .*
- (e) *If $F/K(x)$ is finite and K infinite, then there exists a finite separable extension N_0/K such that if $N_0 \subseteq N$, then the embedding problem (μ, β) splits.*

Proof. Let F_0 be the fixed field of $\ker \gamma$. Then γ induces an isomorphism $\bar{\gamma}: \text{Gal}(F_0/K(x)) \rightarrow B$. Thus, the following commutative diagram (recall that α is the restriction map) implies that (ν, β) is rational.

$$\begin{array}{ccccc}
 \text{Gal}(F/K(x)) & \xrightarrow{\text{res}} & \text{Gal}(F_0/K(x)) & & \\
 & \searrow \gamma & \downarrow \bar{\gamma} & \searrow \text{res} & \\
 & & B & \xrightarrow{\beta} & \text{Gal}(L/K)
 \end{array}$$

Now under these identifications, $\gamma\Phi^* = (\Phi|_{F_0})^*$, and hence is a geometric weak solution.

To see (c), recall the natural isomorphism

$$\text{Gal}(FN/K(x)) \cong \text{Gal}(F/K(x)) \times_{\text{Gal}(L/K)} \text{Gal}(N/K) = C$$

is given by $\sigma \mapsto (\sigma|_F, \sigma|_N)$.

Part (d) is immediate since the correlation $\Phi \mapsto \Phi^*$ respects restrictions, and since ϵ is the restriction map.

To prove (e), choose $a \in K$ such that $(x-a)$ is unramified in F . Extend the specialization $x \mapsto a$ to a place φ of F/L . Let N_0 be the residue field of F under φ . Then φ^* is a geometric weak solution of (ν, α) that factors via $\text{Gal}(N_0/K)$. Choose N as in (c) with $N_0 \subseteq N$. We need to show that $\beta: C \rightarrow \text{Gal}(N/K)$ splits.

Indeed, let $\beta': \text{Gal}(N/K) \rightarrow C$ be defined as follows. For each $\sigma \in \text{Gal}(N/K)$ we write $\varphi^*(\sigma) = \varphi^*(\sigma')$, where $\sigma' \in \text{Gal}(K)$ is an extension of σ to K_s . Since φ^* factors via $\text{Gal}(N_0/K)$ it also factors via $\text{Gal}(N/K)$, and hence $\varphi^*(\sigma)$ is well defined. Now we set $\beta'(\sigma) = (\varphi^*(\sigma), \sigma)$. Clearly β' is a section of β , as needed. \square

2.3. Characterization of fully Hilbertian fields. We start by formulating the Hilbertianity property in terms of geometric solutions of rational embedding problems.

Proposition 2.13. *A field K is Hilbertian if and only if every rational embedding problem is geometrically solvable.*

Proof. We can assume that K is infinite.

Assume that every rational embedding problem is geometrically solvable. Let $f(X, Y) \in K[X, Y]$ be an irreducible polynomial that is separable in Y and with a leading coefficient $a(X) \neq 0$. Choose some finite set $A \subseteq K$ with more elements than the numbers of roots of a .

Let x be a variable, take F to be the splitting field of $\prod_{\alpha \in A} f(x + \alpha, Y)f(\frac{1}{x} + \alpha, Y)$ over $K(x)$, and let $L = F \cap K_s$. Let Φ^* be a geometric solution of the rational embedding problem

$$(\nu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K)).$$

Assume without loss of generality that $\beta = \Phi(x) \in K$ (otherwise we repeat the following argument with $\beta = \Phi(\frac{1}{x})$). Since $|A|$ is bigger than the number of roots of $a(x)$, there exists $\alpha \in A$ for which $a(\beta + \alpha) \neq 0$. Let $y \in F$ be a root of $f(x + \alpha, Y)$ and let $\gamma = \Phi(y)$. Then γ is finite. But since Φ^* is surjective, $[F : K(x)] = [\bar{F} : K]$. In particular

$$\deg_Y f(x + \alpha, Y) = [K(x, y) : K(x)] = [K(\gamma), K],$$

and thus $f(\beta + \alpha, Y)$ is irreducible (recall that $f(\beta + \alpha, \gamma) = 0$).

Next assume that K is Hilbertian and consider a rational finite embedding problem

$$(\nu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K)).$$

Let $f(x, Y) \in K[x, Y]$ be an irreducible polynomial that is separable in Y , a root of which generates $F/K(x)$. Let $0 \neq g(x) \in K[x]$ be the product of the discriminant of f over $K(x)$ and its leading coefficient. Choose an irreducible specialization $x \mapsto \alpha \in K$ of $f(x, Y)$ such that $g(\alpha)$ does not vanish.

Extend this specialization to an L -place of F . Then Φ is unramified over $K(x)$. Moreover, since $f(\alpha, Y)$ is irreducible, we have that $[\bar{F} : K] = [F : K(x)]$. Thus the decomposition group equals $\text{Gal}(F/K(x))$, i.e., Φ^* is surjective. \square

Remark 2.14. In the above result, it is necessary that the solutions are geometric. Indeed, there exists a non-Hilbertian field K whose absolute Galois group is ω -free (i.e., every finite embedding problem is solvable): Let $K_0 = \mathbb{C}(x)$, then $\text{Gal}(K_0)$ is an infinitely generated free group. The restriction map $\alpha: \text{Gal}(K_0((x))) \rightarrow \text{Gal}(K_0)$ splits ([8, Corollary 4.1(e)]). Let K be the fixed field of the image of a section of α . Then $\text{Gal}(K) \cong \text{Gal}(K_0)$ is free of infinite rank. But K is Henselian as an algebraic extension of the Henselian field $K_0((x))$. By [6, Lemma 15.5.4] K is not Hilbertian.

We wish to characterize fully Hilbertian fields in terms of geometric solutions of rational embedding problems. In the meanwhile we shall define *Galois fully Hilbertian* fields to be fields with the proper amount of geometric solutions to a rational embedding problem. Moreover we shall require that the solutions are independent in the following sense. Then we shall prove that Galois fully Hilbertian fields, regular fully Hilbertian fields and fully Hilbertian fields are the same.

Definition 2.15. We call a family of solutions $\{\theta_i \mid i \in I\}$ of a non-trivial embedding problem (1) **independent** (or **linearly disjoint**) if the solution fields, i.e. the fixed fields of $\ker \theta_i$, are linearly disjoint over L .

Remark 2.16. The name derives from the group theoretic analog, cf. [4, Definition 2.3].

Before continuing, we strengthen Lemma 2.12 and show that independency of solutions is preserved under mild changes of the embedding problems.

Lemma 2.17. *In the notation of Lemma 2.12 the following extra assertions hold:*

- (a) *Let $\{\Phi_i^* \mid i \in I\}$ be a family of independent geometric solutions of (ν, α) . Then $\{\gamma\theta_i \mid i \in I\}$ is a family of independent geometric solutions of (ν, β) .*
- (b) *If $\{\theta_i \mid i \in I\}$ is a set of independent geometric solutions of (μ, β) , then $\{\epsilon\theta_i \mid i \in I\}$ is a set of independent geometric solutions of (ν, α) .*

Proof. We start with the first case. Let \bar{F}_i be the residue field of Φ_i . By assumptions, $\{\bar{F}_i \mid i \in I\}$ is a linearly disjoint set over L . Let \bar{E}_i be the residue field of F_0 under $\Phi_i|_{F_0}$. (Recall that $B \cong \text{Gal}(F_0/K(x))$.) Then $\bar{E}_i \subseteq \bar{F}_i$, and hence $\{\bar{E}_i \mid i \in I\}$ is a linearly disjoint set over L . Thus, by definition, $\gamma\Phi_i^* = (\Phi_i|_{F_0})^*$ are independent solutions of (ν, β) .

Next we prove the second case. Denote by G, B, A the groups $\text{Gal}(F/K(x)), \text{Gal}(N/K), \text{Gal}(L/K)$, respectively. By [4, Lemma 2.5], for any $i_1, \dots, i_n \in I$, the image of $\theta_{i_1} \times \dots \times \theta_{i_n}$ is the fiber product C_B^n of n copies of C over B . Hence by [4, Lemma 2.4] the image of the corresponding $\epsilon\theta_{i_1} \times \dots \times \epsilon\theta_{i_n}$ equals the fiber product G_A^n of n copies of G over A , and thus $\{\epsilon\theta_i \mid i \in I\}$ is an independent set of solutions, by [4, Lemma 2.5]. By Lemma 2.12 these solutions are geometric. \square

Definition 2.18. A field K is called **Galois fully Hilbertian** if every non-trivial rational finite embedding problem for K has $|K|$ independent geometric solutions.

Remark 2.19. Note that the definition of Galois fully Hilbertian is equivalent to saying that the property of fully Hilbertian fields holds for all irreducible $f(X, Y) \in K[X, Y]$ that are Galois over $K(X)$.

Remark 2.20. Finite fields are not Galois fully Hilbertian, since the absolute Galois group of a finite field is pro-cyclic.

The requirement on the solutions in the definition of Galois fully Hilbertian fields can be weakened, as we show in the next lemma.

Lemma 2.21. *A field K is Galois fully Hilbertian if and only if every non-trivial rational finite split embedding problem for K has $|K|$ pairwise-independent geometric solutions.*

Proof. We may assume that K is infinite. Consider a rational embedding problem

$$\begin{array}{ccc} & \text{Gal}(K) & \\ & \downarrow \nu & \\ \text{Gal}(F/K(x)) & \xrightarrow{\alpha} & \text{Gal}(L/K). \end{array}$$

Let N_0 be as in Lemma 2.12(e). Choose some finite Galois extension N/K that contains LN_0 . Then Lemma 2.17 implies that it suffices to find a set of m independent geometric solutions of the rational finite split embedding problem (μ, β) , where $\mu: \text{Gal}(K) \rightarrow \text{Gal}(N/K)$ is the restriction map, and

$$\beta: \text{Gal}(F/K(x)) \times_{\text{Gal}(L/K)} \text{Gal}(N/K) \rightarrow \text{Gal}(N/K)$$

is the quotient map of the fiber product.

By assumption there exists a set of pairwise-independent geometric solutions $\{\theta_i \mid i \in I\}$ of (μ, β) with $|I| = |K|$. By [4, Proposition 3.6] there exists a subset $I' \subseteq I$ of the same cardinality $|I'| = |K|$ for which $\{\theta_i \mid i \in I'\}$ is an independent set of geometric solutions, as needed. \square

Standard set theoretic considerations show that it suffices to solve infinite embedding problems of cardinality $< |K|$.

Lemma 2.22. *For a field K to be Galois fully Hilbertian it suffices that any rational embedding problem (1) in which $\text{rank Gal}(F/K(x)) < |K|$ and $\ker \alpha$ is finite is geometrically solvable.*

Proof. Consider a rational finite embedding problem

$$(\nu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K))$$

for K and write $B = \text{Gal}(F/K(x))$ and $A = \text{Gal}(L/K)$. In particular F is regular over L .

For each $i < m$ we inductively construct a geometric solution θ_i such that the corresponding solution field N_i is linearly disjoint of the compositum $\prod_{j < i} N_j$ over L . This would imply that $\{\theta_i \mid i < m\}$ is a family of independent geometric solutions, and hence the proof.

Assume we have constructed geometric solutions θ_j for each $j < i$ that are independent. Let N_j be the solution field of θ_j , let $B_j = \text{Gal}(N_j/K)$. Then $B \cong B_j$.

Write $N = \prod_{j < i} N_j$ and let $\nu_i: \text{Gal}(K) \rightarrow \text{Gal}(N/K)$ be the restriction map. Since the $\{\theta_j \mid j < i\}$ are independent it follows that $\text{Gal}(N/K)$ is canonically isomorphic to the fiber product $\prod_A B_j$ of B_j over A , where $j < i$. The isomorphism is given by $\sigma \mapsto ((\sigma|_{N_j}))_{j < i}$ [4, Lemma 2.5].

Moreover, since F is regular over L , it is linearly disjoint of N , and hence of $N(x)$ over $L(x)$. Hence

$$\text{Gal}(FN/K(x)) \cong \text{Gal}(F/K(x)) \times_{\text{Gal}(L/K)} \text{Gal}(N/K) \cong B \times_A \left(\prod_{j < i} B_j \right),$$

so $\text{rank Gal}(FN/K(x)) \leq i + 1 < m$. Let $\alpha_i: \text{Gal}(FN/K(x)) \rightarrow \text{Gal}(N/K)$ be the restriction map.

The assumption gives a geometric solution $\Phi^*: \text{Gal}(K) \rightarrow \text{Gal}(FN/K(x))$ of the rational embedding problem

$$(\nu_i: \text{Gal}(K) \rightarrow \text{Gal}(N/K), \alpha_i: \text{Gal}(FN/K(x)) \rightarrow \text{Gal}(N/K)).$$

Let M and N_i be the residue fields of FN and F under Φ , respectively, and let $\varphi_i = \Phi|_F$.

Then $\theta_i = \varphi_i^* : \text{Gal}(K) \rightarrow \text{Gal}(F/K(x))$ is a geometric solution. Since the residue field of $N(x)$ is N and Φ^* is an isomorphism, we have $[M : N] = [FN : N(x)] = |B|/|A|$. But $M = NN_i$; so $[NN_i : N] = |B|/|A| = [N_i : L]$. Therefore N_i is linearly disjoint of N over L , as required. \square

We are now ready to prove that the notions of Galois fully Hilbertian fields, regular fully Hilbertian fields, and fully Hilbertian fields are equivalent.

Theorem 2.23. *Let K be a field. The following conditions are equivalent.*

- (a) K is fully Hilbertian.
- (b) K is regular fully Hilbertian.
- (c) K is Galois fully Hilbertian.

Proof. It is clear that full Hilbertianity implies regular full Hilbertianity.

Assume K is regular fully Hilbertian. We prove that K is Galois fully Hilbertian. Let

$$(\nu : \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha : \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K))$$

be a rational non-trivial finite split embedding problem. By Lemma 2.21 it suffices to find $|K|$ independent geometric solutions of (n_0, α_0) . By Zorn's lemma there exists a maximal set of geometric independent solutions $\{\theta_i \mid i \in I\}$ of (ν, α) . We claim that $|I| = |K|$. Assume otherwise, i.e., $|I| < |K|$.

Let N be the compositum of the fixed fields of $\ker \theta_i$, $i \in I$. Since $|I| < |K|$ the rank of $\text{Gal}(N/K)$ is less than $|K|$. Thus

- (2) there exist at most $|I|$ finite subextensions of N/K .

By assumption α splits, let $\alpha' : \text{Gal}(L/K) \rightarrow \text{Gal}(F/K(x))$ be a section of α and let E be the fixed field of the image of α' . Then $EL = F$ and $E \cap L = K$. In particular E/K is regular. Choose a primitive element $y \in E$ of $E/K(x)$ that is integral over $K[x]$. Then $E = K(x, y)$ and the irreducible polynomial $f(x, Y) \in K[x, Y]$ of y over $K(x)$ is monic and absolutely irreducible.

Since K is regular fully Hilbertian there exists a set $A \subseteq H(f)$ of cardinality $|A| = |K|$ and a choice of roots \bar{y}_a of $f(a, Y)$ such that the fields $E_a = K(\bar{y}_a)$ are linearly disjoint over K . In particular $E_a \cap E_b = K$ for all $a \neq b$.

We claim that there exist infinitely many $a \in A$ such that $E_a \cap N = K$, and hence E_a and N are linearly disjoint over K (recall that N/K is Galois). Otherwise, we would have that $E'_a = E_a \cap N \neq K$ (where a runs on a co-finite subset of A) are $|K|$ finite subextensions of N/K . Since

$$K \subseteq E'_a \cap E'_b \subseteq E_a \cap E_b \subseteq K,$$

it follows that $E'_a \cap E'_b = K$, hence E'_a, E'_b are distinct. This contradicts (2).

Choose $a \in A$ such that E_a and N are linearly disjoint and if φ is a place of F that lies over $(x - a)$, then $\bar{F} = \overline{EL} = \bar{E}L = E_a L$. Since E_a and L are also linearly disjoint, we have

$$[\bar{F} : K] = [E_a L : K] = [E_a : K][L : K] = [E : K(x)][L(x) : K(x)] = [F : K(x)],$$

hence $\varphi^*: \text{Gal}(K) \rightarrow \text{Gal}(F/K(x))$ is surjective. Now E_a, N are linearly disjoint over K , hence \bar{F}, N are linearly disjoint over L . But this means that $\{\varphi^*, \theta_i\}$ is a set of geometric independent solutions, a contradiction to the maximality of $\{\theta_i \mid i \in I\}$.

It remains to prove that a Galois fully Hilbertian field K is fully Hilbertian. Let $f(X, Y)$ be an irreducible polynomial that is separable in Y . Let x be a variable, and let y be a root of $f(x, Y)$ in some fixed algebraic closure of $K(x)$. Let $E = K(x, y)$. Then $E/K(x)$ is a finite separable extension. Let $L_0 = E \cap K_s$.

Choose a Galois extension $F/K(x)$ such that $E \subset F$ and let $L = F \cap K_s$. Then $EL \subseteq F$ and, since E is regular over L_0 ,

$$(3) \quad [EL : L] = [E : L_0].$$

Since K is Galois fully Hilbertian, it follows that there exists a family $\{\varphi_i^* \mid i \in I\}$ of independent geometric solutions of the non-trivial finite rational embedding problem $(\mu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K))$, and $|I| = |K|$. The set of $i \in I$ for which one of the following conditions is not satisfied is finite, hence we can assume that every $i \in I$ satisfies these conditions.

- (a) $a_i = \varphi_i(x)$ and $b_i = \varphi(y_i)$ are finite, for all $i \in I$.
- (b) $f(a_i, b_i) = 0$.
- (c) The residue field of E under φ_i is $\bar{E}_i = K(b_i)$.
- (d) The residue field of EL under φ_i is $\overline{EL}_i = \bar{E}_i L = L(b_i)$.

Since φ_i^* is surjective for all $i \in I$, we have $[\bar{F}_i : K] = [F : K(x)]$, and hence $[\bar{R}_i : \bar{S}_i]$ for any tower $K(x) \subseteq S \subseteq R \subseteq F$. Hence to finish the proof, it suffices to prove that the \bar{E}_i are linearly disjoint over L_0 , for any finite subset J of I .

Let J be a finite subset of I . Since $\{\varphi_i^* \mid i \in J\}$ are independent, the fields $\bar{F}_i, i \in J$ are linearly disjoint over L . In particular $\bar{E}_i L$ are linearly disjoint over L . By (3) we have

$$\begin{aligned} [E : L_0]^{|J|} &= \prod_{i \in J} [E : L_0] = \prod_{i \in J} [\bar{E}_i : L_0] \geq [\prod_{i \in J} \bar{E}_i : L_0] \geq [\prod_{i \in J} (\bar{E}_i L) : L] \\ &= \prod_{i \in J} [\bar{E}_i L : L] = \prod_{i \in J} [EL : L] = [EL : L]^{|J|} = [E : L_0]^{|J|}. \end{aligned}$$

We thus get that all inequalities are equalities, and thus \bar{E}_i are linearly independent over L_0 . \square

For countable fields, Hilbertianity is the same as full Hilbertianity. This is an immediate consequence of Proposition 2.13 and Lemma 2.22.

Corollary 2.24. *Let K be a countable field. Then K is Hilbertian if and only if K is fully Hilbertian.*

2.4. The absolute Galois group of fully Hilbertian fields. In this section we consider the group theoretic properties of the absolute Galois group of fully Hilbertian fields.

Recall the definition of semi-free groups [4].

Definition 2.25. A profinite group Γ of infinite rank m is called **semi-free** if every finite split embedding problem for Γ has a set of m independent solutions.

The following conjecture is the analog of Conjecture “Split EP/ K_{hilb} .” of [5].

Conjecture 2.26. The absolute Galois group of a fully Hilbertian field K is semi-free of rank $|K|$.

In [5] Dèbes and Deschamps show that “Split EP/ K_{hilb} .” follows from the conjecture they call “Split EP/ $k(t)$.” We show that a slightly stronger property implies Conjecture 2.26.

Proposition 2.27. *Let K be a fully Hilbertian field and assume that any finite split embedding problem for K is equivalent to a rational embedding problem. Then $\text{Gal}(K)$ is semi-free of rank $|K|$.*

Proof. Any split embedding problem over K is equivalent to a rational embedding problem. Therefore, by definition there exist $|K|$ independent geometric solutions. \square

Recall that a field K is called **ample** (or **large**) if every curve defined over K with a simple K -rational point has infinitely many K -rational points. In [19], Pop proves that the assumption of Proposition 2.27 holds for an ample field, see also [11]. Therefore we get:

Corollary 2.28. *Let K be a fully Hilbertian ample field. Then $\text{Gal}(K)$ is semi-free of rank $|K|$.*

A stronger property than being ample is being PAC: A field K is PAC if every curve defined over K has infinitely many K -rational points. The next result extends Roquette’s Theorem [6, Corollary 27.3.3].

Proposition 2.29. *Let K be a PAC field. Then K is fully Hilbertian if and only if $\text{Gal}(K)$ is free of rank $|K|$.*

Proof. Assume K is fully Hilbertian. Then Corollary 2.28 implies that $\text{Gal}(K)$ is semi-free of rank $|K|$. But [6, Theorem 11.6.2] implies that $\text{Gal}(K)$ is projective, and thus $\text{Gal}(K)$ is free of rank $|K|$ [4, Theorem 3.5].

Assume that $\text{Gal}(K)$ is free of rank $|K|$. Then any finite embedding problem has m independent solutions [6, Proposition 25.1.6]. Since K is PAC, any solution of a geometric embedding problem is geometric [2, Corollary 3.4]. Therefore any rational finite embedding problem for K has m independent geometric solutions, i.e., K is fully Hilbertian. \square

We now consider arbitrary fields. We give a result about embedding problems with abelian kernel.

Proposition 2.30. *Let K be a fully Hilbertian field of cardinality m , A an abelian group, L/K a finite Galois extension with Galois group $G = \text{Gal}(L/K)$. Assume that G acts on A . Then the infinite group $A^m \rtimes G$ occurs as a Galois group over K . In particular A^m occurs as a Galois group over K .*

Proof. Let $\mu: \text{Gal}(K) \rightarrow G$ be the restriction map, and $\alpha: A \rtimes G \rightarrow G$ the quotient map. By Ikeda’s theorem [6, Proposition 16.4.4], the embedding problem (μ, α) is equivalent to a rational embedding problem. Since K is fully Hilbertian, there exists a set S of m independent solutions.

The fiber product of m copies of $A \rtimes G$ over G is isomorphic to $A^m \rtimes G$ [4, Lemma 4.3] and the corresponding solution

$$\prod_{\theta \in S} \theta: \text{Gal}(K) \rightarrow A^m \rtimes G$$

is surjective [4, Lemma 2.5]. □

For any field K , the rank of $\text{Gal}(K)$ is bounded by $|K|$. Taking $A = \mathbb{Z}/2\mathbb{Z}$ in Proposition 2.30, we get the following result:

Proposition 2.31. *If K is fully Hilbertian, then the rank of $\text{Gal}(K)$ equals $|K|$.*

3. RATIONAL FUNCTION FIELDS

In this section we show that the basic families of Hilbertian fields — number fields and function fields — are fully Hilbertian. Since for a countable field full Hilbertianity is equivalent to Hilbertianity, we are left with function fields over an infinite field. Our proof is based on an explicit description of elements in Hilbert sets and on the fact that full Hilbertianity is preserved by finite extensions. The latter assertion will be proved below, see Corollary 5.2.

Let K_0 be an infinite field and $K = K_0(t)$ a rational function field over K_0 . Then each Hilbert set contains a set

$$\{a + bt \mid g(a, b) \neq 0\},$$

for some nonzero polynomial $g(A, B) \in K_0[A, B]$ [6, Proposition 13.2.1]. In this section we use this description in order to show that K is fully Hilbertian.

Theorem 3.1. *Let K_0 be a field and let $K = K_0(t)$ be a rational function field. Then K is fully Hilbertian.*

Proof. If K_0 is countable, then Hilbertianity is the same as fully Hilbertianity. Hence K is fully Hilbertian.

Assume that $m = |K_0|$ is infinite. By Lemma 2.22 it suffices to geometrically solve a rational embedding problem

$$(\nu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K))$$

under the assumption that $\text{rank Gal}(F/K(x)) = n < m$.

Since the number of finite subextensions of $F/K(x)$ is bounded by n (and actually equals n if n is infinite), we can order the finite subextensions $E \neq K(x)$ of $F/K(x)$, say $\{E_i \mid i \leq n\}$. For each E_i there exists a Hilbert set H_i such that for each $u \in H_i$ and for each K -place φ of E_i that lies over $(x - u)$ the degree of the residue field extension equals to $[E_i : K(x)]$. In particular φ is unramified in E_i .

Let $g_i(A, B) \in K_0[A, B]$ be the nonzero polynomial such that $\{a + bt \mid a, b \in K_0 \text{ and } g(a, b) \neq 0\} \subseteq H_i$. Write $C_i(K_0) = \{(a, b) \in K_0^2 \mid g(a, b) = 0\}$ for the corresponding curve. Now since $n < m$

$$K_0^2 \neq \bigcup_{i \leq n} C_i(K_0).$$

Let $(a, b) \in K_0^2 \setminus \bigcup_{i \leq n} C_i(K_0)$. Extend the specialization $x \mapsto a + bt \in K$ to a K -place φ of F .

For each $i \leq n$, $g_i(a, b) \neq 0$, hence $\varphi|_{E_i}$ is unramified over $K(x)$. Therefore φ is unramified over K , and thus the geometric weak solution $\varphi^*: \text{Gal}(K) \rightarrow \text{Gal}(F/K(x))$ of (ν, α) is well defined.

We claim that $\varphi^*: \text{Gal}(K) \rightarrow \text{Gal}(F/K(x))$ is a solution, i.e., surjective. To show that it suffices to show that $D_\varphi = \text{Gal}(F/K(x))$, where D_φ is the corresponding decomposition group. Let Δ be the decomposition field (i.e. the fixed field of D_φ in F). We need to show that $\Delta = K(x)$.

If $\Delta \neq K(x)$, then there exists a finite extension E_i of $K(x)$ such that $E_i \subseteq \Delta$. Hence the residue field \bar{E}_i of E_i is K . But since $g_i(a, b) \neq 0$ we have $[\bar{E}_i : K] = [E_i : K(x)] > 1$.

This contradiction implies that $\Delta = K(x)$, and hence φ^* is an epimorphism, which concludes the proof. \square

Corollary 3.2 (Theorem 1.2). *Let F be a finitely generated transcendental extension of an arbitrary field K . Then F is fully Hilbertian.*

Proof. Let (t_1, \dots, t_r) be a transcendence basis of F/K . Then F is a finite extension of $K_0(t_1, \dots, t_r)$. By Theorem 3.1 the field $K(t_1, \dots, t_r) = K(t_1, \dots, t_{r-1})(t_r)$ is fully Hilbertian. By Corollary 5.2 below, $F/K(t_1, \dots, t_r)$ is fully Hilbertian. \square

4. THE TWINNING PRINCIPLE

We mentioned in the introduction the *twinning principle* formulated by Lubotzky-Jarden. This principle suggests there should be a connection between results about free subgroups of a free profinite group and results about Hilbertian separable extensions of a Hilbertian field. We also remarked in the introduction that the *Haran-Shapiro induction* gives a strong evidence to this principle, since it proves the diamond theorem in both settings, and the proofs are analogous.

In fact results about Hilbertian fields transfer to results about free profinite groups of countable rank, using Roquette's theorem, see [15, Weak twinning principle].

In this section we further study the twinning principle. We first claim that the connection should be between semi-free profinite groups of rank m and fully Hilbertian fields of cardinality m .

- (a) The connection is evident from the characterization of fully Hilbertian fields as Galois fully Hilbertian fields (Theorem 2.23). A semi-free group Γ of rank m is a profinite group for which every non-trivial finite split embedding problem has m independent solutions, while a Galois fully Hilbertian field of cardinality $|K| = m$ is a field for which every non-trivial *rational* embedding problem has m independent *geometric* solutions.
- (b) The absolute Galois group of a fully Hilbertian field is not projective in general, and free groups are projective. In the meanwhile semi-free groups are, in a sense, free group without projectivity ([4, Theorem 3.5]).
- (c) A fully Hilbertian ample field has a semi-free group rank $|K|$ (Corollary 2.28), and conditionally this is always the case (Proposition 2.27).

Maybe the most convincing argument for this connection is the following

- (d) The proofs about sufficient conditions for a subgroup of a semi-free group to be semi-free carry over to the field theoretic setting.

Remark 4.1. If one wants to consider the more classical setting of Hilbertian fields, then our method gives the connection with the property that each finite split embedding problem has a solution. One can even consider only semi-free groups of countable rank.

Let us go into more details. First note that there is a certain trade-off here – in the group theoretic setting we need to solve all finite split embedding problems, while in field theory only rational embedding problems come into the picture. On the other hand, in the field theoretic setting we need the solution to have an extra property, namely only geometric solutions are considered.

The way we transfer group theoretic proofs into field theory is via the Haran-Shapiro induction. This method uses fiber products and twisted wreath products in order to induce solutions of embedding problems from the group to its subgroup. So what we need to do is to prove, or essentially to observe, that all constructions of the Haran-Shapiro induction are field theoretic constructions. That is to say, (1) if one starts from a rational embedding problem, then the constructed embedding problems are also rational (2) the solutions induced by the constructions preserve the property of being geometric.

As an immediate consequence of this, all the permanence properties of semi-free groups carry over to fully Hilbertian fields. In particular we get all cases of Theorem 1.4.

4.1. Fiber products and twisted wreath products. As indicated before in results about semi-free subgroups of semi-free groups there are two group theoretic constructions involved, fiber products and twisted wreath products. Let us start with the more elementary one, fiber products.

Write $\Gamma = \text{Gal}(K)$ and consider an embedding problem $(\mu: \Gamma \rightarrow G, \alpha: H \rightarrow G)$ for K . Let Δ be a normal subgroup of Γ contained in $\ker \mu$. Then μ factors as $\mu = \bar{\mu}\hat{\mu}$, where $\hat{\mu}: \Gamma \rightarrow \hat{G} := \Gamma/\Delta$ is the quotient map and $\bar{\mu}: \hat{G} \rightarrow G$ is canonically defined. This data defines a corresponding **fiber product embedding problem**:

$$\begin{array}{ccc} & & \Gamma \\ & & \downarrow \hat{\mu} \\ H \times_G \hat{G} & \xrightarrow{\hat{\alpha}} & \hat{G} \\ \downarrow \beta & & \downarrow \bar{\mu} \\ H & \xrightarrow{\alpha} & G \end{array}$$

Here $H \times_G \hat{G} = \{(h, \hat{g}) \in H \times \hat{G} \mid \alpha(h) = \bar{\mu}(\hat{g})\}$ and $\hat{\alpha}, \beta$ the canonical projections.

A (weak) solution $\hat{\theta}: \Gamma \rightarrow H \times_G \hat{G}$ of the fiber product embedding problem induces the (weak) solution $\theta = \beta\hat{\theta}$ of (μ, α) .

The following result asserts that this construction preserves field theoretic aspects.

Lemma 4.2. *In the above notation, if (μ, α) is geometric, then so is $(\hat{\mu}, \hat{\alpha})$. Moreover, if $\hat{\theta}$ is geometric, so does θ .*

More precisely, assume $H = \text{Gal}(F/K(x))$, $G = \text{Gal}(L/K)$ for $L = F \cap K_S$, and α, μ are the restriction maps. Let N be the fixed field of Δ . Then $\hat{G} = \text{Gal}(N/K)$, $H \times_G \hat{G} = \text{Gal}(FN/K(x))$, and $\hat{\alpha}, \beta$ are the corresponding restriction maps. Moreover, if $\hat{\theta} = \hat{\mathfrak{P}}^$ for some unramified prime extension $\hat{\mathfrak{P}}/(x-a)$ of $FN/K(x)$, then $\theta = (\mathfrak{P} \cap F)^*$.*

Proof. See [2, Lemma 2.6]. \square

Now we move to the more sophisticated construction of twisted wreath products. For the reader's convenience we give a short survey on the Haran-Shapiro induction, starting from the definitions. See [4] for full details and proofs.

Definition 4.3. Let $A, G_0 \leq G$ be finite groups. Assume that G_0 acts on A (from the right). Let

$$\text{Ind}_{G_0}^G(A) = \{f: G \rightarrow A \mid f(\sigma\rho) = f(\sigma)^\rho, \forall \sigma \in G, \rho \in G_0\} \cong A^{(G:G_0)}.$$

Then G acts on $\text{Ind}_{G_0}^G(A)$ by $f^\sigma(\tau) = f(\sigma\tau)$. We define the **twisted wreath product** to be the semidirect product

$$A \text{ wr}_{G_0} G = \text{Ind}_{G_0}^G(A) \rtimes G,$$

i.e., an element in $A \text{ wr}_{G_0} G$ can be written uniquely as $f\sigma$, where $f \in \text{Ind}_{G_0}^G(A)$ and $\sigma \in G$. The multiplication is then given by $(f\sigma)(g\tau) = fg^{\sigma^{-1}}\sigma\tau$. The twisted wreath product is equipped with the quotient map $\alpha: A \text{ wr}_{G_0} G \rightarrow G$ defined by $\alpha(f\sigma) = \sigma$.

The map $\pi: \text{Ind}_{G_0}^G(A) \rtimes G_0 \rightarrow A \rtimes G_0$ defined by $\pi(f\sigma) = f(1)\sigma$ is called the **Shapiro map**. It is an epimorphism, since, for $f \in \text{Ind}_{G_0}^G(A)$ and $\sigma \in G_0$, we have

$$\pi(f^\sigma) = f(\sigma) = f(1)^\sigma = \pi(f)^\sigma.$$

Definition 4.4. A tower of fields

$$K \subseteq L_0 \subseteq L \subseteq F \subseteq \hat{F}$$

is said to **realize** the twisted wreath product $A \text{ wr}_{G_0} G$ if \hat{F}/K is a Galois extension with Galois group isomorphic to $A \text{ wr}_{G_0} G$ and the tower of fields corresponds to the subgroups (via taking fixed fields in \hat{F})

$$A \text{ wr}_{G_0} G \geq \text{Ind}_{G_0}^G(A) \rtimes G_0 \geq \text{Ind}_{G_0}^G(A) \geq \ker \pi \geq 1.$$

We note that the extension F/L_0 is Galois with group $A \rtimes G_0$, and the restriction map $\text{Gal}(\hat{F}/L_0) \rightarrow \text{Gal}(F/L_0)$ is the corresponding Shapiro map of $A \text{ wr}_{G_0} G$. For more details see [6, Remark 13.7.6] or [10, Remark 1.2].

Let $\Lambda \leq \Gamma$ be profinite groups. Consider a finite split embedding problem $(\mu_1: \Lambda \rightarrow G_1, \beta_1: A \rtimes G_1 \rightarrow G_1)$ for Λ . To use the Haran-Shapiro induction, first we choose an open normal subgroup Δ of Γ such that $\Delta \cap \Gamma \leq \ker \mu_1$. Let $\mu: \Gamma \rightarrow G := \Gamma/\Delta$ be the quotient

map and $\mu_0 = \mu|_{\Lambda} : \Lambda \rightarrow G_0 := \Lambda/\Lambda \cap \Delta$. Then μ_1 factors as $\mu_1 = \bar{\mu}_1 \mu_0$. Moreover we have the following embedding problems

$$(4) \quad \begin{array}{ccc} \text{Ind}_{G_0}^G(A) \rtimes G_0 & \xrightarrow{\beta} & G_0 \\ \downarrow \pi & & \downarrow \mu_0 \\ A \rtimes G_0 & \xrightarrow{\beta_0} & G_0 \\ \downarrow \rho & & \downarrow \bar{\mu}_1 \\ A \rtimes G_1 & \xrightarrow{\beta_1} & G_1 \end{array} \quad \begin{array}{ccc} & & \Gamma \\ & & \downarrow \mu \\ A \text{ wr}_{G_0} G & \xrightarrow{\alpha} & G. \end{array}$$

μ_1

Here β is the restriction of α to $\text{Ind}_{G_0}^G(A) \rtimes G_0$, π is the Shapiro map, $A \rtimes G_0 \cong (A \rtimes G_1) \times_{G_1} G_0$, and ρ, β_0 are the projection maps. Note the the lower square in the left diagram is the fiber product embedding problem.

Now, if $\theta : \Gamma \rightarrow A \text{ wr}_{G_0} G$ is a weak solution, then $\theta_0 = \rho\pi\theta|_{\Lambda}$ is a weak solution of the original embedding problem (μ_1, β_1) . The problem here is that if θ is a solution, i.e., surjective, it does not imply that θ_0 is a solution. So we are lead to Haran's contribution to the method: Under some conditions on the subgroup Λ (e.g., open, $\Gamma' \leq \Lambda$, or most generally, contained in a diamond) the Haran-Shapiro induction gives that, taking Δ small enough, or equivalently, G large enough, we have

$$\theta \text{ surjective} \implies \theta_0 \text{ surjective.}$$

Moreover, if $\{\theta_i \mid i \in I\}$ is a family of pairwise-independent solutions of (μ, α) , then the induced solutions $\{\theta_{i0} \mid i \in I\}$ of (μ_1, β_1) are also pairwise-independent.

Now we show that these constructions carry over to the field theoretic setting. For this assume that M is a separable extension of an *infinite* field K , $\Gamma = \text{Gal}(K)$, and $\Lambda = \text{Gal}(M)$. Also denote by L the fixed field of Δ , i.e., $G = \text{Gal}(L/K)$.

Lemma 4.5. *If (μ_1, β_1) is a rational embedding problem for M , then there exists a finite separable extension K'/K such that if $K' \subseteq L$, then all the embedding problems in (4) are rational, and all maps are restriction maps. Moreover, if a weak solution θ of (μ, α) is geometric, then the induced weak solution $\theta_0 = \rho\pi\theta|_{\text{Gal}(M)}$ of (μ_1, β_1) is also geometric.*

More precisely, assume that $A \rtimes G_1 = \text{Gal}(F_1/M(x))$, $G_1 = \text{Gal}(N_1/M)$ for $N_1 = F_1 \cap M_s$, and β_1, μ_1 are the restriction maps. Then there exists a finite separable extension K'/K such that for every finite Galois extension L of K that contains K' we have:

(a) $N_1 \subseteq ML$.

Let $L_0 = L \cap M$ and $G_0 = \text{Gal}(ML/L) \cong \text{Gal}(L/L_0)$.

(b) *There exist $x_0 \in L_0(x)$ such that $L_0(x_0) = L_0(x)$ and a tower of fields*

$$K(x_0) \subseteq L_0(x) \subseteq L(x) \subseteq F \subseteq \hat{F}$$

that realizes $A \text{ wr}_{G_0} G$. In particular, we identify $\text{Gal}(\hat{F}/K(x_0)) = A \text{ wr}_{G_0} G$.

- (c) \hat{F} is regular over L .
 (d) Let $\hat{F}_0 = \hat{F}M$, $F_0 = FM$, and $N_0 = LM$. Then N_0/L , $\hat{F}_0/M(x)$, and $F_0/M(x)$ are Galois, we have

$$\begin{aligned}\mathrm{Gal}(N_0/M) &\cong G_0, \\ \mathrm{Gal}(\hat{F}_0/M(x)) &\cong \mathrm{Ind}_{G_0}^G(A) \rtimes G_0, \\ \mathrm{Gal}(F_0/M(x)) &\cong A \rtimes G_0,\end{aligned}$$

and under these identification the maps in (4) are the restriction maps.

- (e) Let $\theta: \mathrm{Gal}(K) \rightarrow A \mathrm{wr}_{G_0} G$ be a geometric weak solution, i.e., $\theta = \hat{\varphi}^*$ for some place $\hat{\varphi}$ of \hat{F} that is unramified over $K(x)$, and extends a specialization $x \mapsto a \in K$. Extend $\hat{\varphi}$ to an M -place $\hat{\psi}$ of \hat{F}_0 . Then $\theta_0 := \rho\pi\theta|_{\mathrm{Gal}(M)} = (\hat{\psi}|_{F_1})^*$.

Proof. Since the restriction map $\mathrm{Gal}(F_1/M(x)) \rightarrow \mathrm{Gal}(N_1/M)$ splits, we can lift $G_1 = \mathrm{Gal}(N_1/M)$ to a subgroup of $\mathrm{Gal}(F_1/M(x))$. Let E be its fixed field. Then $E \cap N_1 = M$ and $EN_1 = F_1$. Let $y \in E$ be a primitive element of $E/M(x)$, i.e., $E = M(x, y)$. Then y is also a primitive element of $F_1/N_1(x)$. Then the irreducible polynomial $f(x, Y) \in M[x, Y]$ of y over $M(x)$ is Galois over $N_1(x)$.

Let K'/K be a finite extension such that $N_1 \subseteq MK'$, the coefficients of $f(x, Y)$ are in $K' \cap M$, and $f(x, Y)$ is Galois over $K'(x)$. Let L be a finite Galois extension of K that contains K' . Then, in particular, (a) holds, $f(x, Y) \in L_0[x, Y]$ for $L_0 = L \cap M$, and $f(x, Y)$ is Galois over $L(x)$. Choose a basis c_1, \dots, c_n of L_0/K and let x_0, x_1, \dots, x_n be an $(n+1)$ -tuple of variables.

Now by [10, Lemma 3.1] there exist fields F', \hat{F}' such that (denoting $\mathbf{x} = (x_1, \dots, x_n)$)

$$K(\mathbf{x}) \subseteq L_0(\mathbf{x}) \subseteq L(\mathbf{x}) \subseteq F' \subseteq \hat{F}'$$

realizes $A \mathrm{wr}_{G_0} G$ and \hat{F}' is regular over L . Furthermore, F' is generated by a root of $f(\sum_{i=1}^n c_i x_i, Y)$ over $L(\mathbf{x})$.

A usual combination of the Bertini-Neother Lemma and the Matsusaka-Zariski Theorem (see, e.g., [3, Lemma 2.4]) implies that we can substitute x_i with $\alpha_i + \beta_i x_0$ for some $\alpha_i, \beta_i \in K^\times$ and extend this substitution to a K -place of \hat{F}' with residue field \hat{F} with the same properties. That is, if we denote by F the residue field of F' , then

$$K(x_0) \subseteq L_0(x_0) \subseteq L(x_0) \subseteq F \subseteq \hat{F}$$

realizes $A \mathrm{wr}_{G_0} G$, \hat{F} is regular over L , and F is generated by a root of $f(\sum_{i=1}^n c_i(\alpha_i + \beta_i x_0), Y) \in L_0[x_0, Y]$ over $L(x_0)$. Since c_1, \dots, c_n are linearly independent over K , we have that $\sum_{i=1}^n \beta_i c_i \neq 0$. Therefore $u = \sum_{i=1}^n c_i(\alpha_i + \beta_i x_0)$ is a transcendental element and $L_0(x_0) = L_0(u)$. We may apply an isomorphism that sends u to x to assume that

$$K(x_0) \subseteq L_0(x) \subseteq L(x) \subseteq F \subseteq \hat{F}$$

realizes $A \mathrm{wr}_{G_0} G$, \hat{F} regular over L , and F is generated by the root y of $f(x, Y)$. This finishes the proof of (b) and (c).

Let $N_0 = ML$, $F_0 = FM$, $\hat{F}_0 = \hat{F}L$, as in (d). Note that $F_0 = FM = K(x, y)LM = \hat{N}_0(x, y)$. Since \hat{F} is regular over L , we have $L_0 = \hat{F} \cap M = L \cap M$, and thus $\text{Gal}(N_0/M) \cong \text{Gal}(L/L_0) = G_0$. Similarly we have

$$\text{Gal}(\hat{F}_0/M(x)) \cong \text{Gal}(\hat{F}/L_0(x)) \cong \text{Ind}_{G_0}^G(A) \rtimes G_0$$

and $\text{Gal}(F_0/M(x)) \cong \text{Gal}(F/L_0(x)) \cong A \rtimes G_0$. Since all isomorphisms are defined canonically, the maps in (4) are the restriction maps.

It remains to prove (e). Let $\hat{\varphi}^*: \text{Gal}(K) \rightarrow \text{Gal}(\hat{F}/K(x))$ be a weak geometric solution. Extend $\hat{\varphi}$, M -linearly, to a place $\hat{\psi}$ of \hat{F}_0 . Then $\hat{\psi}$ is unramified over $M(x)$, and $\hat{\varphi}^*|_{\text{Gal}(M)} = \hat{\psi}^*$. Moreover, since all maps in (4) are the restriction maps, we get that $\rho\pi(\hat{\varphi}^*|_{\text{Gal}(M)}) = \rho\pi(\hat{\psi}^*) = (\hat{\psi}|_{F_1})^*$. \square

4.2. Separable extensions of fully Hilbertian fields. The following result is more general than Theorem 1.4, cf. Main Theorem of [4].

Theorem 4.6. *Let M be a separable extension of a fully Hilbertian field K . Then each of the following conditions suffices for M to be fully Hilbertian.*

- (a) $[M : K] < \infty$.
- (b) The Galois group Γ of the Galois closure of M/K is finitely generated.
- (c) The cardinality of the set of all finite subextensions of M/K is less than $|M|$.
- (d) M is a proper finite extension of a Galois extension N/K .
- (e) M is an abelian extension of K .
- (f) There exist Galois extensions M_1, M_2 of K such that $M \subseteq M_1M_2$, but $M \not\subseteq M_i$ for $i = 1, 2$.
- (g) M is contained in a Galois extension N/K with pronilpotent group and $[M : K]$ is divisible by at least two primes.
- (h) M/K is sparse.
- (i) $[M : K] = \prod p^{\alpha(p)}$, where $\alpha(p) < \infty$ for all p .

Proof. Let $m = |K|$ and $(\mu_1: \text{Gal}(M) \rightarrow \text{Gal}(N_1/M), \alpha: \text{Gal}(F_1/M(x)) \rightarrow \text{Gal}(N_1/M))$ be a rational split embedding problem for M . Then if we write $G_1 = \text{Gal}(N_1/M)$, then $\text{Gal}(F_1/M(x)) \cong A \rtimes G_1$ and α the quotient map. It suffices to find a set of m pairwise-independent geometric solutions of (μ_1, β_1) .

Let K'/K be the finite separable extension given in Lemma 4.5. Choose a ‘large’ finite Galois extension L/K such that $K' \subseteq L$ and let $\mu: \text{Gal}(K) \rightarrow G := \text{Gal}(L/K)$ be the restriction map. In the notation of Lemma 4.5 the embedding problem

$$(\mu: \text{Gal}(K) \rightarrow G, \alpha: A \text{wr}_{G_0} G \rightarrow G)$$

is rational, and hence has a set of m independent geometric solutions $\{\theta_i \mid i \in I\}$ of (μ, α) .

Cases (a) and (b): Note that (a) is a special case of (b). In [4, Section 5.1.2] it is proved that there exists an open normal subgroup Λ of $\text{Gal}(K)$ (in the notation of loc. cit. $L = \Lambda$) such that if $\text{Gal}(L) \leq \Lambda$, then $S = \{\rho\pi\theta_i \mid i \in I\}$ is a set of pairwise-independent solutions of (μ_1, β_1) . Choose L sufficiently large, so that it contains both K' and the fixed field of Λ .

Then on the one hand S is a set of pairwise-independent solutions and on the other hand the solutions in S are geometric (Lemma 4.5).

Case (f): As in the previous case, in [4, Section 5.1.3] it is proved, basing on the proof of [6, Theorem 25.4.3], that there exists a normal subgroup Λ of $\text{Gal}(K)$ such that if $\text{Gal}(L) \leq \Lambda$, then S (as above) is a set of pairwise-independent solutions of (μ_1, β_1) . Hence the same argument as above finishes the proof.

The proof of all the other cases other follows from the above cases, as shown in [4] or proved in a similar manner. \square

Remark 4.7. In the proof above, the only new property we exploited is that the constructions of fiber products and twisted wreath product, and the induced solutions, are field theoretic.

5. PURELY INSEPARABLE EXTENSIONS

In the previous section we dealt with separable extensions of a fully Hilbertian field, using the twinning principle. Here we show that full Hilbertianity, as Hilbertianity, is preserved under purely inseparable extensions. This will be useful later, for example in order to prove that full Hilbertianity is preserved under all finite extensions.

Proposition 5.1. *Let K be a fully Hilbertian field and E/K a purely inseparable extension. Then E is fully Hilbertian.*

Proof. Let $(\nu: \text{Gal}(E) \rightarrow \text{Gal}(M/E), \alpha: \text{Gal}(P/E(x)) \rightarrow \text{Gal}(M/E))$ be a rational embedding problem for E . Since E/K is purely inseparable and $F/E(x)$, M/E are Galois, the extensions $F/K(x)$, M/K are normal. Let F (resp. L) be the maximal separable extension of $K(x)$ (resp. K) in P (resp. M). Then $P = FE$ and $M = LE$.

$$\begin{array}{ccccc} E(x) & \text{---} & M(x) & \text{---} & P \\ | & & | & & | \\ K(x) & \text{---} & L(x) & \text{---} & F \end{array}$$

Then P/F and M/L are purely inseparable and $\text{Gal}(F/K(x)) \cong \text{Gal}(P/E(x))$, $\text{Gal}(L/K) \cong \text{Gal}(M/E)$ via the restriction maps.

Note that $P = FE$ is regular over E , i.e., linearly disjoint of the algebraic closure \tilde{E} of E over E . As F/K is separable and E/K purely inseparable, F and E are linearly disjoint over K . Thus F and $\tilde{E}(= \tilde{K})$ are linearly disjoint. Thus F is regular over K .

Let $\mu: \text{Gal}(K) \rightarrow \text{Gal}(L/K)$ and $\beta: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K)$ be the restriction maps. As K is fully Hilbertian, there exists a set $\{\varphi_i^* \mid i \in I\}$ of independent solutions of (μ, β) with $|I| = |K|$. Extend E -linearly each φ_i to a place ψ_i of P . Since $\mu = \nu \text{res}_{E_s, K_s}$ and $\beta = \alpha \text{res}_{P, F}$, and since the restriction maps $\text{res}_{E_s, K_s}: \text{Gal}(E) \rightarrow \text{Gal}(K)$, $\text{res}_{P, F}: \text{Gal}(P/E(x)) \rightarrow \text{Gal}(F/K(x))$ are isomorphisms, we get that $\{\psi_i^* \mid i \in I\}$ is a set of independent solutions of (ν, α) of cardinality $|I| = |K| = |E|$. \square

Corollary 5.2. *A finite extension of a fully Hilbertian field is fully Hilbertian.*

Proof. Let L/K be a finite extension. Let E the maximal purely inseparable extension of K inside L . Then L/E is separable. By Proposition 5.1 E is fully Hilbertian and by Theorem 4.6 L is fully Hilbertian. \square

6. DOMINATING EMBEDDING PROBLEMS

This section provides some auxiliary results that reduce the necessary embedding problems needed for full Hilbertianity. This reduction is needed in the sequel in order to prove Theorem 1.5.

6.1. Hurwitz's Formula. Let F/E be a finite separable extension of function fields over a base field L . Denote by g_F, g_E the genera of F, E , respectively, and let $n = [F : E]$. Hurwitz's formula asserts that

$$(5) \quad 2g_F - 2 = n(2g_E - 2) + \deg R,$$

where R is the ramification divisor. If the characteristic of L is $p > 0$, then the primes of F divide into two sets: the tamely ramified primes $P_{tr} = \{\mathfrak{P} \mid p \nmid e_{\mathfrak{P}}\}$ and the wildly ramified primes $P_{wr} = \{\mathfrak{P} \mid p \mid e_{\mathfrak{P}}\}$. If the characteristic of L is 0, then all the primes are, by definition, tamely ramified. We have

$$(6) \quad \deg R = \sum_{\mathfrak{P} \in P_{tr}} (e_{\mathfrak{P}} - 1) + \sum_{\mathfrak{P} \in P_{wr}} l_{\mathfrak{P}},$$

and $l_{\mathfrak{P}} > e_{\mathfrak{P}} - 1$, see [13, Corollary IV.2.4].

If \mathfrak{p} is a prime of $L(x)/L$, then either \mathfrak{p} corresponds to some irreducible polynomial in $L[x]$, in this case we say that \mathfrak{p} is finite (w.r.t. x), or \mathfrak{p} corresponds to ∞ , and then we write $\mathfrak{p} = \mathfrak{p}_{\infty}$.

The following result is an immediate consequence of Hurwitz's formula.

Corollary 6.1. *Let $F/L(x)$ be a separable extension of degree $n \geq 2$. Assume that all primes of F lying above \mathfrak{p}_{∞} are tamely ramified in F . Then there exists a prime \mathfrak{P} of F lying over a finite prime \mathfrak{p} of $L(x)$ such that $\mathfrak{P}/\mathfrak{p}$ is ramified.*

Proof. By (5) we have

$$2g_F - 2 = -2n + \deg R \Rightarrow \deg R = 2g_F + 2(n - 1) \geq 2(n - 1) > n - 1.$$

(Recall that $n \geq 2$.) Using the formula $\sum_{\mathfrak{P}/\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} = n$ with $\mathfrak{p} = \mathfrak{p}_{\infty}$ we get

$$\sum_{\mathfrak{P}/\mathfrak{p}_{\infty}} (e_{\mathfrak{P}} - 1) \leq n - 1 < \deg R.$$

Thus there must be a prime \mathfrak{P} of F not lying above \mathfrak{p}_{∞} that is ramified. \square

Lemma 6.2. *Let L be a field and let $F/L(x)$ be a finite Galois extension that is not wildly ramified at infinity. Suppose $F/L(x)$ is regular, and that $\text{Ram}(F/L(x)) = \{c_1, c_2, \dots, c_k\} \subseteq L$. For each $1 \leq i \leq k$ let $\mathfrak{P}_{i,1}, \dots, \mathfrak{P}_{i,g_i}$ be the primes of F lying over $(x - c_i)$. Denote the inertia group of $F/L(x)$ at $\mathfrak{P}_{i,j}$ by $I_{i,j}$. Then G is generated by all the $I_{i,j}$.*

Proof. Let $H \leq G$ be the subgroup generated by all $I_{j,j}$. Let $E = F^H$ the corresponding field. Then, by definition, E is ramified at most at infinity, and this ramification, if exists, is tame. Thus by Corollary 6.1, $E = L(t)$, i.e., $H = G$. \square

Before we continue we recall some notation. Fix a field L . Let $a \in \tilde{L}$, $f(X)$ its irreducible polynomial over L , and \mathfrak{p} the prime of $L(x)$ that is defined by f . We say that a is a **ramification point** of $F/L(x)$ if \mathfrak{p} is ramified in F . We denote by $\text{Ram}(F/L(x)) \subseteq \tilde{L}$ the set of all ramification points of $F/L(x)$ in \tilde{L} . We emphasize that $\text{Ram}(F/L(x))$ depends on x .

Let $\mathfrak{P}/\mathfrak{p}$ be an extension of primes of $F/L(x)$ with ramification index e . If the characteristic of L is positive, say $p > 0$, we write $e = e'q$, where $\gcd(e', p) = 1$ and q is a power of p . We will call e' the **tame ramification index** of $\mathfrak{P}/\mathfrak{p}$ and q the **wild ramification index**. If L is of characteristic 0, then the tame ramification index equals the ramification index, and the wild ramification index is 1.

If $F/L(x)$ is Galois, then the tame and wild ramification indices are independent of the choice of the prime \mathfrak{P} that lies over \mathfrak{p} , so we abbreviate and say tame (resp., wild) ramification index of \mathfrak{p} in F .

Lemma 6.3. *Let K be an infinite field, let $F_0/K(x_0)$ be a finite Galois extension, and let $L_0 = \tilde{K} \cap F_0$. Assume that $\text{Ram}(F_0/L_0(x_0)) \subseteq K_s$. Then there exist $x \in K(x_0)$ and a finite Galois extension $F/K(x)$ such that, for $L = K_s \cap F$, the following conditions hold:*

- (a) $K(x) = K(x_0)$.
- (b) The prime \mathfrak{p}_∞ of $L(x)$ is tamely ramified in F .
- (c) $F_0 \subseteq F$,
- (d) $\text{Ram}(F/L(x)) \subseteq L$.
- (e) Let $c \in \text{Ram}(F/L(x))$, \mathfrak{P}_c a prime of F lying above $\mathfrak{p}_c = (x - c)$, and e' (resp., q) be the tame (resp., wild) ramification index of $\mathfrak{P}_c/\mathfrak{p}_c$. Then
 - (e1) $(x - c)^{1/e'} \in F$,
 - (e2) the primitive e' -th root of unity $\zeta_{e'}$ is contained in L , and
 - (e3) the residue field of F at \mathfrak{P}_c is a purely inseparable extension of L .

Proof. Since K is infinite, there is a Möbius transformation that sends x_0 to $x = \frac{u+vx_0}{w+zx_0}$,

for some $\begin{pmatrix} u & v \\ w & z \end{pmatrix} \in \text{PSL}_2(K)$ under which ∞ is mapped to an unramified point. Clearly $K(x) = K(x_0)$ and $\text{Ram}(F_0/L_0(x)) \subseteq K_s$.

Let $n = |\text{Ram}(F_0/L_0(x))|$, write $\text{Ram}(F_0/L_0(x)) = \{c_1, \dots, c_n\}$, and for each i , let e'_i , (resp., q_i) be the tame (resp., wild) ramification index of $(x - c_i)$ in F_0 . Then $e_i = e'_i q_i$, $i = 1, \dots, n$ are the corresponding ramification indices. Let L be a finite Galois extension of K that contains L_0, c_1, \dots, c_n .

Write $F_1 = F_0 L$. Then $\text{Ram}(F_1/L(x)) = \{c_1, \dots, c_n\}$, and each c_i has the same ramification indices e_1, \dots, e_n (since $L(x)/L_0(x)$ is unramified). Let $F = F_1((x - c_i)^{1/e'_i} \mid i = 1, \dots, n)$. By [6, Example 2.3.8] it follows that F/F_1 is unramified over the primes of F_1 that lie above $(x - c_i)$, $i = 1, \dots, n$. By the multiplicity of ramification indices, we get that each $(x - c_i)$ has ramification e_i in F .

On the other hand, let $\mathfrak{p} \neq (x - c_i)$, $i = 1, \dots, n$ be a finite prime of $L(x)$. Then \mathfrak{p} is unramified both in $F_1/L(x)$ and in $K((x - c_j)^{1/e'_i} \mid i = 1, \dots, n)$. Thus it is unramified in their compositum F . Replace L with a larger extension, if necessary, to assume that the residue field of F w.r.t. \mathfrak{P}_{c_i} is a purely inseparable extension of L .

Finally note that the ramification of \mathfrak{p}_∞ in F divides $e'_1 \cdots e'_n$, and hence is co-prime to the characteristic of K , if not 0. \square

Proposition 6.4. *Let K be an infinite field and*

$$(\mu_0: \text{Gal}(K) \rightarrow \text{Gal}(L_0/K(x_0)), \alpha_0: \text{Gal}(F_0/K(x_0)) \rightarrow \text{Gal}(L_0/K(x_0)))$$

a non-trivial rational finite embedding problem. Then there exist $x \in K(x_0)$ and a non-trivial rational finite embedding problem

$$(\mu: \text{Gal}(K) \rightarrow \text{Gal}(L/K(x)), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K(x)))$$

satisfying Properties (a)-(e) of Lemma 6.3 such that an independent set $\{\theta_i \mid i \in I\}$ of proper geometric solutions of (μ, α) induces an independent set $\{\text{res}_{F, F_0} \theta_i \mid i \in I\}$ of proper geometric solutions of (μ_0, α_0) .

Proof. Let F be the field given by Lemma 6.3. Consider the commutative diagram

$$\begin{array}{ccccc} & & & \text{Gal}(K) & \\ & & & \downarrow \mu & \\ \text{Gal}(F/K(x)) & \xrightarrow{\gamma} & \text{Gal}(F_0 L/K(x)) & \xrightarrow{\beta} & \text{Gal}(L/K) \\ & & \downarrow \pi & & \downarrow \mu' \\ & & \text{Gal}(F_0/K(x)) & \xrightarrow{\alpha_0} & \text{Gal}(L_0/K) \end{array}$$

α (dotted arrow from $\text{Gal}(F/K(x))$ to $\text{Gal}(F_0 L/K(x))$)

μ_0 (curved arrow from $\text{Gal}(L/K)$ to $\text{Gal}(L_0/K)$)

in which all the maps are the restriction maps. We are given an independent set $\{\theta_i \mid i \in I\}$ of geometric proper solutions of (μ, α) .

By Lemma 2.17 $\{\gamma\theta_i \mid i \in I\}$ is an independent set of geometric proper solutions of (μ, β) . Then Lemma 2.17 implies that $\{\pi\gamma\theta_i \mid i \in I\}$ is an independent set of geometric proper solutions of (μ_0, α_0) . \square

The following is an immediate conclusion.

Corollary 6.5. *For a field K to be fully Hilbertian it suffices that every non-trivial rational embedding problem*

$$(\mu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K))$$

satisfying Properties (a)-(e) of Lemma 6.3 has $|K|$ independent geometric solutions.

6.2. Wild ramification. This part deals with wild ramifications. The reader interested only with fields of characteristic zero can skip this part.

For the rest of this section fix a field E with positive characteristic $p > 0$ which is equipped with a discrete valuation v .

Lemma 6.6 (Artin-Schreier theory). *Let F/E be a Galois extension of degree p . There exists $a_0 \in E$ such that for every $a \in a_0 + E^p - E$ and every x satisfying $x^p - x = a$ we have $F = E(x)$.*

Proof. Let $\wp(x) = x^p - x$. Then the short exact sequence

$$0 \longrightarrow \mathbb{F}_p \longrightarrow E_s \xrightarrow{\wp} E_s \longrightarrow 0$$

of additive $\text{Gal}(E)$ -modules gives rise to the following exact sequence of cohomology

$$E \xrightarrow{\wp} E \longrightarrow H^1(\mathbb{F}_q) \longrightarrow H^1(E_s).$$

By Hilbert's 90th, $H^1(E_s) = 0$. Since $\text{Gal}(E)$ acts trivially on $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ we have $H^1(\mathbb{F}_q) = \text{Hom}(\text{Gal}(E), \mathbb{Z}/p\mathbb{Z})$. Therefore $\text{Hom}(\text{Gal}(E), \mathbb{Z}/p\mathbb{Z}) \cong E/\wp(E)$. Applying this to the restriction map $\text{Gal}(E) \rightarrow \text{Gal}(F/E)$ proves the assertion. \square

We give a criterion for v to be totally ramified in a Galois p extension.

Proposition 6.7. *Let F/E be a Galois extension of degree p . Then v is totally ramified in F if and only if there exists $a \in E$ and $x \in F$ such that $F = E(x)$, $x^p - x = a$, and $p \nmid v(a) < 0$.*

Proof. First assume there exist $x \in F$ and $a \in E$ as in the proposition. Let w be a normalized discrete valuation of F lying above v . Then $w(x) < 0$, since otherwise $v(a) \geq 0$. We thus get that $w(x^p) < w(x)$, hence

$$e(w/v)v(a) = w(a) = w(x^p - x) = w(x^p) = pw(x).$$

Since $\gcd(v(a), p) = 1$, we get that p divides $e(w/v)$, hence $p = e(w/v)$. Thus v is totally ramified in each F .

Conversely, assume that v is totally ramified in F and let w be its normalized extension. Fix $1 \leq i \leq m$. We show how to choose suitable a, x . Choose a uniformizer $\pi \in E$ for v , i.e., $v(\pi) = 1$. Then $w(\pi) = p$. Let K be the residue field of E . Since w/v is totally ramified, K is the residue field of F as well. Let φ be the corresponding place of F .

Apply Lemma 6.6 to get an element $a_0 \in E$ such that for every $a \in a_0 + E^p - E$ and $x \in F$ such that $x^p - x = a$ we have $F = E(x)$. Denote $A = a_0 + E^p - E$. By [6, Example 2.3.9] $v(A)$ is a set of negative integer numbers. Let $l \in \mathbb{N}$ be minimal such that $-lp \in v(A)$. Choose some $a \in A$ satisfying $v(a) = -lp$. It suffices to show that $-lp \neq \max v(A)$.

Let $x \in F$ be a root of $X^p - X = a$. Then $F = E(x)$. We have $w(x^p - x) = w(a) = pv(a) < 0$. Hence $w(x) < 0$, so $w(x^p) < w(x)$ which implies $pw(x) = w(x^p) = w(x^p - x) = pv(a)$. Therefore $w(x) = v(a) = -lp$.

Write $a = \pi^{-lp}\alpha$ and $x = \pi^{-l}\xi$. Note that $v(\alpha) = v(a) + lp = 0$ and $w(\xi) = w(x) + lw(\pi) = -lp + lp = 0$. Thus α, ξ are w -invertible, or equivalently, $\bar{\alpha}, \bar{\xi} \neq 0, \infty$, where the notation $\bar{\cdot}$ indicates the image after applying φ . We apply φ to the equation

$$\xi^p - x\pi^{lp} = x^p\pi^{lp} - x\pi^{lp} = a\pi^{lp} = \alpha$$

to get the equality $\bar{\xi}^p = \bar{\alpha}$. Since $\bar{E} = K$, there exists $b \in E$ with $\bar{b} = \bar{\xi}$. In particular $v(b) = 0$. Also, as $\bar{b}^p - \bar{\alpha} = 0$, we have $v(b^p - \alpha) > 0$. Let $a' = a - \pi^{-lp}b^p + \pi^{-l}b \in A$.

Then $d := v(a - \pi^{-lp}b^p) = v(-\pi^{-lp}(\alpha - b^p)) = -lp + v(\alpha - b^p) > -lp$. Thus $v(a') \geq \min\{d, -m\} > -lp = v(a)$. This implies $v(a) \neq \max v(A)$, as needed. \square

Now we are ready to state and prove the main result of this part which sets a necessary condition for a totally ramified Galois extension of order a power of p to remain totally ramified when moving to the residue extension w.r.t. some other place.

Corollary 6.8. *Let N/E be a Galois extension of degree a power of p . Let v be a discrete valuation of E that is totally ramified in N . Let φ be a place of N , let \bar{N}, \bar{E} be the respective residue fields of N, E under φ , and assume the characteristic of \bar{E} is p and \bar{N}/\bar{E} is a Galois extension of degree $[\bar{N} : \bar{E}] = [N : E]$. Then there exists $a_1, \dots, a_m \in E$ with $v(a_i) < 0$ and $\gcd(v(a_i), p) = 1$ for each $1 \leq i \leq m$, such that for every discrete valuation \bar{v} of \bar{E} , if $\bar{a}_i := \varphi(a_i) \neq \infty$, $\bar{v}(\bar{a}_i) < 0$ and $\gcd(\bar{v}(\bar{a}_i), p) = 1$ for each $1 \leq i \leq m$, then \bar{v} is totally ramified in \bar{N} .*

Proof. Let F_1, \dots, F_m be all the minimal extension of E inside N . Then F_i/E is a Galois extension of degree p . Proposition 6.7 gives $a_1, \dots, a_m \in E, x_1 \in F_1, \dots, x_m \in F_m$ such that $F_i = E(x_i)$, $x_i^p - x_i = a_i$, $v(a_i) < 0$ and $\gcd(v(a_i), p) = 1$, for each $1 \leq i \leq m$.

Let \bar{F} be the residue field of F under φ . By assumption \bar{N}/\bar{E} is a Galois extension of the same degree as N/E , hence $\text{Gal}(\bar{N}/\bar{E}) \cong \text{Gal}(N/E) = G$. Thus $\text{Gal}(\bar{N}/\bar{F}) = \Phi$. Let H be the inertia group of \bar{v} (w.r.t. some extension of it to \bar{N}) in G , and let \bar{E}' be its fixed field. Then, by definition \bar{v} is unramified in \bar{E}' .

If $\bar{E}' \neq \bar{E}$, then \bar{E}' contains some \bar{F}_i . Since \bar{a}_i is finite, so is \bar{x}_i , $\bar{F}_i = \bar{E}_i(\bar{x}_i)$, and $\bar{x}_i^p - \bar{x}_i = \bar{a}_i$. Proposition 6.7 implies that \bar{v} is totally ramified in \bar{F}_i , hence ramified in \bar{E}' . This contradiction implies that $\bar{E}' = \bar{E}$, i.e., \bar{v} is totally ramified in \bar{N} . \square

7. COMPLETE DOMAINS

We now prove Theorems 1.5 and 1.7 about quotient fields of complete local domains. To get independent solutions of a rational embedding problem we show that if a in a Hilbert set approximates all the ‘ramification points’ of the embedding problem w.r.t. some valuations of our base field K , then the geometric inertia groups become inertia groups w.r.t. those valuations of K .

Lemma 7.1. *Let L be a field, let $E/L(t)$ be a finite separable extension, and let $\beta_1, \dots, \beta_l \in E$. Let $\mathfrak{P}/(t-c)$ be a prime extension of $E/L(t)$ such that $e(\mathfrak{P}/(t-c)) = f(\mathfrak{P}/(t-c)) = 1$. Then there exists a finite set $\Lambda \subseteq L$, such that for any discrete valuation v of L , satisfying $v(\lambda) = 0$ for each $\lambda \in \Lambda$, there exists $M \in \mathbb{R}$ such that for every $\alpha \in L$ satisfying $v(\alpha - c) > M$ the following properties hold:*

- (a) *There exists a prime \mathfrak{P}_α of E lying over $(t - \alpha)$ such that v is unramified in the residue field \bar{E}_α .*
- (b) *Let v_s be an extension of v to L_s . Let m_i be the order of β_i at \mathfrak{P} and let $\nu \in \mathbb{Z}$ be co-prime to m_i , for each $1 \leq i \leq l$. Suppose $m_i < 0$ for each $1 \leq i \leq l$. Then if $v(\alpha - c)$ is co-prime to ν , then $v_s(\bar{\beta}_i) \in \mathbb{Z}$, $v_s(\bar{\beta}_i) < 0$ and $\gcd(v_s(\bar{\beta}_i), \nu) = 1$, for each $1 \leq i \leq l$. (Here $\bar{\beta}_i$ is the image of β_i modulo \mathfrak{P}_α .)*

Proof. Let $\hat{E} = \hat{E}_{\mathfrak{P}}$ be the completion of E at \mathfrak{P} , and consider the completion $L((t-c))$ of $L(t-c)$ w.r.t. $(t-c)$. Then $\hat{E}/L((t-c))$ is unramified and of residue field degree 1. Hence $\hat{E} = L((t-c))$.

Let $\beta_0 \in E$ be a primitive element of $E/L(t)$. Then $\beta_0, \beta_1, \dots, \beta_l \in L((t-c))$, thus we have

$$\beta_i = \sum_{n=m_i}^{\infty} \lambda_{i,n}(t-c)^n, \quad m_i \in \mathbb{Z}, \lambda_{i,n} \in L,$$

for each $0 \leq i \leq l$. Without loss of generality we can assume that $m_0 > 0$ (by multiplying β_0 with a sufficiently large power of $(t-c)$). Put $\Lambda = \{\lambda_{1,m_1}, \dots, \lambda_{l,m_l}\}$

Suppose v is a discrete valuation of L , satisfying $v(\lambda) = 0$ for each $\lambda \in \Lambda$, and v_s an extension of v to L_s . Let \hat{L} be the completion of L at v , and extend v to the algebraic closure of \hat{L} compatibly with v_s . Since $\beta_i \in L((t-c)) \subseteq \hat{L}(((t-c)))$ is algebraic over $L(t-c) \subseteq \hat{L}(t-c)$ for each $0 \leq i \leq l$, we get by [1, Theorem 2.14] that β_i converges at some $b_i \in \hat{L}$. That is, $v(\lambda_{i,n}b_i^n) = v(\lambda_{i,n}) + nv(b_i) \rightarrow \infty$. Choose $b \in L$ with sufficiently large value $M := v(b)$. That is, we assume that $M \geq \max\{v(b_0), v(b_1), \dots, v(b_l)\}$, and hence $\beta_0, \beta_1, \dots, \beta_l$ converge at b , and for every $r > M, 1 \leq i \leq l$ and $n > m_i$ the following inequality holds.

$$(7) \quad v(\lambda_{i,m_i}) + m_i r < v(\lambda_{i,n}) + nr.$$

Denote $x = \frac{t-c}{b}$. Let $R = \hat{L}\{x\}$ be the ring of convergent power series in x over \hat{L} . That is, all power series in $\hat{L}[[x]]$ whose series of coefficients converges to 0 with respect to v . In particular, $\beta_i = \sum_{n=1}^{\infty} \lambda_{i,n}b^n x^n \in R$, for all $i = 0, 1, \dots, l$.

Now, suppose $\alpha \in L$ satisfies $v(\alpha - c) > M$. Then the element $\varepsilon = \frac{\alpha-c}{b} \in \hat{L}$ satisfies $v(\varepsilon) > 0$. Since \hat{L} is complete with respect to v , we have a substitution homomorphism $\varphi_\alpha: R \rightarrow \hat{L}$, given by $\varphi_\alpha(\sum \mu_n x^n) = \sum \mu_n \varepsilon^n$. Extend φ_α to a place of $Q = \text{Quot}(R)$.

We also have $\varphi_\alpha(\beta_i) = \sum_{n=m_i}^{\infty} \lambda_{i,n}(\alpha - c)^n$. Applying (7) to $r = v(\alpha - c)$ we get that $v(\lambda_{i,m_i}(\alpha - c)^{m_i}) < v(\lambda_{i,n}(\alpha - c)^n)$, for every $n > m_i$. Therefore, if we further assume that $v(\alpha - c)$ is co-prime to ν , then, for all $i \geq 1$,

$$v(\varphi_\alpha(\beta_i)) = v\left(\sum_{n=m_i}^{\infty} \lambda_{i,n}(\alpha - c)^n\right) = v(\lambda_{i,m_i}(\alpha - c)^{m_i}) = m_i v(\alpha - c)$$

is a negative integer (since m_i is negative), co-prime to ν . This concludes the proof of (b).

Let us continue and prove (a). Since $\beta_0 \in R$, the field E is contained in Q . The restriction of φ_α to E fixes L and maps t to α (by the definition of φ_α). Let \mathfrak{P}_α be the corresponding prime of E . Then \mathfrak{P}_α lies over the prime $(t - \alpha)$ of $L(t)$.

By the Weierstrass division theorem for convergent power series, each element of R can be written in the form $g \cdot (x - \varepsilon) + r$, with $g \in R, r \in \hat{L}$. It follows that the kernel of φ_α (as a homomorphism of R) is a principal ideal, generated by $x - \varepsilon$. Moreover, by the Weierstrass preparation theorem for convergent power series, R is a unique factorization domain (whose primes are the primes of $\hat{L}[x]$). Hence each element $h \in Q$ can be written in the form

$(x - \varepsilon)^n \frac{f}{g}$, with $f, g \in R$ not divisible by $x - \varepsilon$, and $n \in \mathbb{Z}$. Then $\varphi_\alpha(\frac{f}{g}) = \frac{\varphi_\alpha(f)}{\varphi_\alpha(g)} \in \hat{L}^\times$. Thus, if $n \geq 0$, then $\varphi_\alpha(h) \in \hat{L}$, and if $n < 0$, then $\varphi_\alpha(h) = \infty$. So the residue field of Q at φ_α is \hat{L} . Thus \bar{E}_α is contained in \hat{L} , hence \bar{E}_α/L is unramified at v . \square

Lemma 7.2. *Let K be a field, let $F/K(x)$ be a finite Galois extension with $L = F \cap K_s$, let $c \in \text{Ram}(F/K(x)) \cap L$, let \mathfrak{P} a prime of F lying above $\mathfrak{p} = (x - c)$, let I be the corresponding inertia group, let e be the ramification index, and let $E = F^I$ the inertia field. Assume conditions (e1)-(e2) of Lemma 6.3 are satisfied and that the residue field of F at \mathfrak{P} is L , in addition to (e3). Then there exists a finite set $\Lambda \subseteq L$, such that if v_s is a valuation of K_s that restricts to a discrete normalized valuation v of K , and satisfies $v(\lambda) = 0$ for each $\lambda \in \Lambda$, then there exists $M \in \mathbb{R}$ such that if $\alpha \in K$ satisfies*

- (a) $v(\alpha - c) > M$,
- (b) $v(\alpha - c)$ is co-prime to e ,
- (c) $(x - \alpha)$ is totally inert in F ,

then $\text{Gal}(\bar{F}/\bar{E})$ is an inertia group of v in \bar{F} , where \bar{F}, \bar{E} are the respective residue fields of F, E at the unique extension \mathfrak{P}_α of $(x - \alpha)$ to F .

Proof. For any separable extension N of K we write v_N for the normalized valuation that lies above v and below v_s . Similarly for every subfield F' of F containing $L(x)$, we let $\mathfrak{P}_{F'}$ be the restriction of \mathfrak{P} to F' .

We recall that $e = e'q$, where e' is the tame ramification index and q is the wild ramification index. If the characteristic of K is 0, then $e' = e$ and $q = 1$, and if the characteristic is $p > 0$, then $\text{gcd}(e', p) = 1$ and $q = p^r$, for some $r \geq 0$.

CONSTRUCTION IN THE WILD RAMIFICATION CASE: The following construction is needed only in the case where $q > 1$. Since I is an inertia group, it has a unique p -syllow subgroup J . Then $J \triangleleft I$, $|J| = q$, $(I : J) = e'$. Let E' be the fixed field of J in F . Then $[F : E'] = q$, $[E' : E] = e'$. Furthermore both $\mathfrak{P}_{E'}/\mathfrak{P}_E$ and $\mathfrak{P}_F/\mathfrak{P}_{E'}$ are totally ramified, while the former ramification is tame and the latter is wild.

Let $a_1, \dots, a_l \in E'$ be the elements that Corollary 6.8 gives when applying it to F/E' (instead of N/E in the notation of the corollary) with the normalized valuation $v_{\mathfrak{P}_{E'}}$ (instead of v) arising from the prime $\mathfrak{P}_{E'}$ and with the place φ arising from the prime \mathfrak{P}_α . Let $m_i = v_{\mathfrak{P}_{E'}}(a_i)$ for each $1 \leq i \leq l$. Then $m_i < 0$ is co-prime to p , for each $1 \leq i \leq l$. Let Λ be the finite set given by Lemma 7.1 (if $q = 1$, Λ may be chosen to be empty). Suppose v satisfies the conditions of the proposition (we fix such v now, even if $q = 1$ and the construction we are making in this part is redundant), and let M be the bound given by Lemma 7.1. Note that $\bar{a}_i := \varphi(a_i)$ is finite for all α but a finite set, hence, without loss of generality, we can assume it is finite (by enlarging M).

Then if

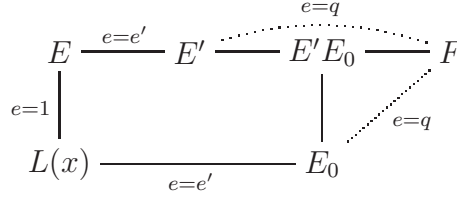
$$(8) \quad p \nmid v_{\bar{E}'}(\bar{a}) < 0,$$

then $v_{\bar{E}'}$ is totally ramified in F . We now prove that (8) holds.

Let $E_0 = L((x - c)^{1/e'})$. We have

$$e'q = e = e(\mathfrak{P}_F/\mathfrak{P}_{E_0})e(\mathfrak{P}_{E_0}/\mathfrak{p}) = e(\mathfrak{P}_F/\mathfrak{P}_{E_0})e',$$

hence $e(\mathfrak{P}_F/\mathfrak{P}_{E_0}) = q$.



Since $e(\mathfrak{P}_{E'E_0}/\mathfrak{P}_{E_0})$ divides $e(\mathfrak{P}_{E'}/\mathfrak{P}_E) = e'$, we get that $\mathfrak{P}_{E'E_0}/\mathfrak{P}_{E_0}$ is unramified. Similarly $\mathfrak{P}_{E'E_0}/\mathfrak{P}_{E'}$ is unramified. Hence m_i is also the order of a_i at $\mathfrak{P}_{E'E_0}$ for each $1 \leq i \leq l$. Since $v(\alpha - c)$ is co-prime to e , it is co-prime to p , hence so is $v((\alpha - c)^{\frac{1}{e'}})$. Lemma 7.1(b), applied to $\beta_i = a_i, t = (x - c)^{1/e'}, \nu = p$ and with c there replaced by 0 here, we get that $v_{\bar{E}'\bar{E}_0}(\bar{a}_i) < 0$ is co-prime to p for each $1 \leq i \leq l$. Since $[\bar{E}'\bar{E}_0 : \bar{E}']$ divides e' which is relatively prime to p , (8) follows. For conclusion, Corollary 6.8 implies that $v_{\bar{E}'}$ is totally ramified in \bar{F} .

CONCLUSION OF THE PROOF: It remains to show that $v_{\bar{E}}/v$ is unramified and that $v_{\bar{E}'}/v_{\bar{E}}$ is totally ramified. The former follows from Lemma 7.1(a) (applied to the prime extension $\mathfrak{P}_E/\mathfrak{p}$ of $E/L(x - c)$).

To prove that $v_{\bar{E}'}/v_{\bar{E}}$ is totally ramified, let $\bar{t} = (\alpha - c)^{1/e'} \in \bar{F}$. Since $v(\alpha - c)$ is co-prime to e' , it is also co-prime to e' . Since

$$\mathbb{Z} \ni v_{\bar{F}}(\bar{t}) = \frac{1}{e'} v_{\bar{F}}(\alpha - c) = \frac{e(v_{\bar{F}}/v)}{e'} v(\alpha - c).$$

we get that $e' \mid e(v_{\bar{F}}/v)$. Note that the condition that $(x - \alpha)$ is totally inert in F means that the degrees of the residue field extensions are preserved. Since $[\bar{F} : \bar{E}'] = q$ is relatively prime to e' and since $v_{\bar{E}}/v$ is unramified, we get that $e' \mid e(v_{\bar{E}'}/v_{\bar{E}})$. On the other hand, $e(v_{\bar{E}'}/v_{\bar{E}}) \leq [\bar{E}' : \bar{E}] = e'$, so $e' = e(v_{\bar{E}'}/v_{\bar{E}})$, i.e., $v_{\bar{E}'}/v_{\bar{E}}$ is totally ramified. \square

Corollary 7.3. *Let K be a Hilbertian field. Consider a rational finite embedding problem $(\mu: \text{Gal}(K) \rightarrow \text{Gal}(L/K), \alpha: \text{Gal}(F/K(x)) \rightarrow \text{Gal}(L/K))$ that satisfies (a)-(e) of Lemma 6.3. For each $c_i \in \text{Ram}(F/L(x))$ let $\mathfrak{P}_{i,1}, \dots, \mathfrak{P}_{i,g_i}$ be the primes of F lying above $\mathfrak{p}_i = (x - c_i)$. Assume that the residue field of F at \mathfrak{P}_c is L .*

Then there exists a finite set $\Lambda \subseteq L$, such that if $\{v_{i,j} \mid 1 \leq i \leq k, 1 \leq j \leq g_i\}$ is a family of non-equivalent discrete valuations of K , totally split in L/K , and trivial on Λ , then there exists a geometric solution \mathfrak{P}^ of (μ, α) with solution field L' , and extensions $v'_{i,j}$ of the $v_{i,j}$ to L' , such that $\text{Gal}(L'/L)$ is generated by the inertia groups of the $v'_{i,j}$ at L'/L .*

Proof. Denote the inertia group of $F/L(x)$ at $\mathfrak{P}_{i,j}$ by $I_{i,j}$. By Lemma 6.2, $\text{Gal}(F/L(x))$ is generated by the $I_{i,j}$.

Let $E_{i,j} = F^{I_{i,j}}$. Then $\mathfrak{p}_{i,j} = \mathfrak{P}_{i,j} \cap E_{i,j}$ is unramified over $L(x)$ and of degree 1. Let $M_{i,j}$ be the bound given by Lemma 7.2 applied to $\mathfrak{p}_{i,j}$, $E_{i,j}$, and $v_{i,j}$. Let $n_{i,j} \in \mathbb{Z}$ be co-prime to e_i and such that $n_{i,j} > M_{i,j}$. Since $v_{i,j}$ totally splits in L/K , K is $v_{i,j}$ -dense in L . Choose $c_{i,j} \in K$ such that $v_{i,j}(c_{i,j} - c_i) > n_{i,j}$.

Since K is Hilbertian, we may choose $\alpha \in K$ such that $(x - \alpha)$ is totally inert in F , or equivalently, the K -specialization $x \mapsto \alpha$ extends to a place \mathfrak{P} of F which defines a geometric solution \mathfrak{P}^* of (μ, α) . Moreover, since Hilbert sets are dense with respect to any finite family of valuations [14, Proposition 19.8], we may assume that $v_{i,j}(\alpha - c_{i,j}) = n_{i,j}$. Hence, $v_{i,j}(\alpha - c_i) = v_{i,j}((\alpha - c_{i,j}) + (c_{i,j} - c_i)) = n_{i,j}$.

By Lemma 7.2, we get that $\text{Gal}(L'/\bar{E}_{i,j}) \cong I_{i,j}$ is the inertia group of $v'_{i,j}/v_{i,j}$ in L' . Thus, since the $I_{i,j}$ generate $\text{Gal}(F/L(x))$, we get that $\text{Gal}(L'/L)$ is generated by the $\text{Gal}(L'/\bar{E}_{i,j})$, as asserted. \square

Proposition 7.4. *Let K be a Hilbertian field, equipped with a family \mathcal{F} of discrete valuations, satisfying:*

- (i) *For each $a \in K^\times$, $v(a) = 0$ for almost all $v \in \mathcal{F}$.*
- (ii) *For each finite separable extension L/K , there exist $|K|$ valuations in \mathcal{F} that totally split in L/K .*
- (iii) *Each $v \in \mathcal{F}$ is trivial on the prime field of K .*

Then the maximal purely inseparable extension K_{ins} of K is fully Hilbertian.

Proof. Let $\kappa = |K|$. Then any algebraic extension of K has cardinality κ . Let

$$(\mu': \text{Gal}(K_{\text{ins}}) \rightarrow \text{Gal}(L'/K_{\text{ins}}), \alpha': \text{Gal}(F'/K_{\text{ins}}(x)) \rightarrow \text{Gal}(L'/K_{\text{ins}}))$$

be a finite rational embedding problem for K . We need to produce κ pair-wise independent geometric solutions of \mathcal{E}_{ins} .

Let K_0 be a finite purely inseparable extension of K . Since K_{ins}/K_0 is purely inseparable, as in the proof of Proposition 5.1, the maximal separable extension F' (resp., L') of $K_0(x)$ (resp., K_0) in F' (resp., L') is a Galois extension, with same Galois group as $\text{Gal}(F'/K(x))$ (resp., $\text{Gal}(L'/K)$). Moreover, that proof shows that a set of κ pair-wise independent geometric solutions of

$$(\mu: \text{Gal}(K_0) \rightarrow: \text{Gal}(L/K_0), \alpha: \text{Gal}(F/K_0(x)) \rightarrow \text{Gal}(L/K_0))$$

gives a set of κ pair-wise independent geometric solutions of (μ', α') . Therefore it suffices to find κ pair-wise independent geometric solutions of (μ, α) .

By Corollary 6.5 we may assume conditions (a)-(e) of Lemma 6.3 hold. Note that condition (e4) gives that the residue field of \mathfrak{P}_c , $c \in \text{Ram}(F/L(x))$ is a purely inseparable extension of L . Thus if we replace K_0 with a sufficiently large finite extension we may assume that this residue field is L .

Since K_0/K is purely inseparable, each $v \in \mathcal{F}$ can be extended uniquely to a discrete valuation v_0 of K_0 . Let $\mathcal{F}_0 = \{v_0 \mid v \in \mathcal{F}\}$. Clearly (i) and (iii) hold for \mathcal{F}_0 . The last assumption (ii) also holds, since if N/K is separable of degree n and $v \in \mathcal{F}$ is totally split in N , i.e., there exist w_1, \dots, w_n lying above v , then the corresponding $v_0 \in \mathcal{F}_0$ is totally split in NK_0 , since $[NK_0 : K_0] = n$, and the extensions of w_1, \dots, w_n to NK_0 lie above v_0 . Thus, without loss of generality, we may assume that $K = K_0$.

Let \mathcal{F}_L be the family of valuations in \mathcal{F} which are totally split in L/K . Then $|\mathcal{F}_L| = \kappa$. Let $\{\theta_\delta \mid \delta \in \Delta\}$ be a maximal family of pairwise-independent geometric solutions of (μ, α) with corresponding solution fields L_i . We wish to show that $|\Delta| = \kappa$.

Suppose $|\Delta| < \kappa$. Each L_δ is defined by a polynomial over K . Adjoining all the coefficients of all these polynomials to the prime field of K , we get that the solutions are defined over a smaller subfield. That is, there exists a field $M \subset K$ with $|M| < \kappa$, such that each L_δ is of the form $M_\delta K$, for some finite Galois extension M_δ of M .

Let $\mathcal{F}' = \{v \in \mathcal{F}_L \mid v(a) = 0 \text{ for all } a \in M^\times\}$. Then $\mathcal{F}_L \setminus \mathcal{F}' = \bigcup_{a \in M^\times} \{v \in \mathcal{F}_L \mid v(a) \neq 0\}$ is of cardinality $|M|$ at most. In particular \mathcal{F}' is infinite. Let Λ be the finite set given in Corollary 7.3. By discarding finitely many valuations, we can assume that each $v \in \mathcal{F}'$ is trivial on Λ .

Choose distinct $v_{i,j} \in \mathcal{F}'$, $1 \leq i \leq k$, $1 \leq j \leq g_i$. Then all the $v_{i,j}$ are trivial on M , hence on all M_i . By [6, Lemma 2.3.6], all of the $v_{i,j}$ are unramified in L_δ/K for each $\delta \in \Delta$.

By Corollary 7.3 there exists a geometric solution \mathfrak{P}^* with residue field L' , and extensions $v'_{i,j}$ -s of the $v_{i,j}$ -s to L' , such that $\text{Gal}(L'/L)$ is generated by the inertia groups of the $v'_{i,j}$ at L'/L . Denote these groups by $I_{i,j}$. It suffices to show that L' is linearly disjoint from each L_δ over L , $\delta \in \Delta$, since then $\{\theta_\delta \mid \delta \in \Delta\}$ is not maximal.

Indeed, let $\delta \in \Delta$, and let $1 \leq i \leq k$, $1 \leq j \leq g_i$. The restriction $\text{Gal}(L'/L) \rightarrow \text{Gal}(L' \cap L_\delta/L)$ maps $I_{i,j}$ into the inertia group of $v'_{i,j}$ at $L' \cap L_\delta/L$. Since $v_{i,j}$ is unramified at L_δ/L , this inertia group is trivial. Hence each element of $I_{i,j}$ fixes $L' \cap L_\delta$. So $I_{i,j} \subseteq \text{Gal}(L'/L' \cap L_\delta)$.

Since the $I_{i,j}$ generate G , $\text{Gal}(L'/L' \cap L_\delta) = G$, hence $L' \cap L_\delta = L$. Thus L' is linearly disjoint from L_δ over L , for each $\delta \in \Delta$, as claimed. \square

Theorem 7.5. *Let K be the quotient field of a complete local domain R of dimension exceeding 1. Then its maximal purely inseparable extension K_{ins} is fully Hilbertian.*

Proof. By Cohen's structure theorem for complete local domains, R is a finite extension of a domain A of the form $K_0[[X_1, \dots, X_n]]$ for some field K_0 , or of the $A = \mathbb{Z}_p[[X_1, \dots, X_n]]$ for some prime integer p . Since $\dim R > 1$, we have $n > 1$ in the first case and $n \geq 1$ in the second case. In both cases, [18, §5] proves the existence of a family of valuations satisfying conditions (a)-(c) of Proposition 7.4. Thus the maximal purely inseparable extension of $\text{Quot}(A)$ is fully Hilbertian. Since K_{ins} is a finite extension of it, K_{ins} is also fully Hilbertian, by Corollary 5.2. \square

Finally, we get Theorem 1.5:

Corollary 7.6. *Let K be the quotient field of a complete local domain R of dimension exceeding 1. Then $\text{Gal}(K)$ is semi-free of rank $|K|$.*

Proof. Since K is the quotient field of a complete domain, every finite split embedding problem over K is regularly solvable, by [17] or [20]. Hence every finite split embedding problem over K_{ins} is regularly solvable. By the preceding theorem K_{ins} is fully Hilbertian, hence Proposition 2.27, $\text{Gal}(K_{ins})$ is semi-free of rank $|K|$. Finally $\text{Gal}(K) \cong \text{Gal}(K_{ins})$ via the restriction map, hence $\text{Gal}(K)$ is semi-free. \square

REFERENCES

1. Emil Artin, *Algebraic numbers and algebraic functions*, Nelson, 1968.
2. Lior Bary-Soroker, *On pseudo algebraically closed extensions of fields*, 2008.

3. Lior Bary-Soroker, *On the characterization of Hilbertian fields*, Int. Math. Res. Not. IMRN (2008), Art. ID rnn 089, 10.
4. Lior Bary-Soroker, Dan Haran, and David Harbater, *Permanence criteria for semi-free profinite groups*, 2008.
5. Pierre Dèbes and Bruno Deschamps, *The regular inverse Galois problem over large fields*, Geometric Galois actions, 2, London Math. Soc. Lecture Note Ser., vol. 243, Cambridge Univ. Press, Cambridge, 1997, pp. 119–138.
6. Michael D. Fried and Moshe Jarden, *Field arithmetic*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2005.
7. Wulf Dieter Geyer and Moshe Jarden, *Fields with the density property*, J. Algebra **35** (1975), 178–189.
8. Wulf-Dieter Geyer and Moshe Jarden, *On the normalizer of finitely generated subgroups of absolute Galois groups of uncountable Hilbertian fields of characteristic 0*, Israel J. Math. **63** (1988), no. 3, 323–334.
9. Dan Haran, *Free subgroups of free profinite groups*, J. Group Theory **2** (1999), no. 3, 307–317.
10. Dan Haran, *Hilbertian fields under separable algebraic extensions*, Invent. Math. **137** (1999), no. 1, 113–126.
11. Dan Haran and Moshe Jarden, *Regular split embedding problems over complete valued fields*, Forum Math. **10** (1998), no. 3, 329–351.
12. David Harbater and Katherine F. Stevenson, *Local Galois theory in dimension two*, Adv. Math. **198** (2005), no. 2, 623–653.
13. Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.
14. Moshe Jarden, *Intersections of local algebraic extensions of a Hilbertian*, Generators and relations in groups and geometries (Lucca, 1990), 343–405, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., **333**, Kluwer Acad. Publ., Dordrecht, 1991.
15. Moshe Jarden and Alexander Lubotzky, *Hilbertian fields and free profinite groups*, J. London Math. Soc. (2) **46** (1992), no. 2, 205–227.
16. Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.
17. Elad Paran, *Split embedding problems over complete domains*, Ann. of Math. (2), to appear.
18. Elad Paran, *Galois theory over complete local domains*, manuscript.
19. Florian Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), no. 1, 1–34.
20. Florian Pop, *Henselian implies large*, manuscript.
21. Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.
22. Helmut Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996, An introduction.

EINSTEIN INSTITUTE OF MATHEMATICS EDMOND J. SAFRA CAMPUS, GIVAT RAM, THE HEBREW UNIVERSITY OF JERUSALEM, JERUSALEM, 91904, ISRAEL

E-mail address: barylior@math.huji.ac.il

SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, RAMAT AVIV, TEL AVIV, 69978, ISRAEL

E-mail address: paranela@post.tau.ac.il